

9-13-00

A

Mail Label No. EL543499998US

09/12/00

jc921 U.S. PRO

**UTILITY PATENT APPLICATION TRANSMITTAL**  
**(Large Entity)**

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Docket No.  
2204/A55

Total Pages in this Submission  
57

jc918 U.S. PRO  
09/12/00

09/12/00

**TO THE ASSISTANT COMMISSIONER FOR PATENTS**

Box Patent Application  
Washington, D.C. 20231

Transmitted herewith for filing under 35 U.S.C. 111(a) and 37 C.F.R. 1.53(b) is a new utility patent application for an invention entitled:

**SYSTEM, DEVICE, AND METHOD FOR CONTROLLING ACCESS IN A MULTICAST COMMUNICATION NETWORK**

and invented by:

**Thomas P. Hardjono**

If a **CONTINUATION APPLICATION**, check appropriate box and supply the requisite information:

☐ Continuation ☐ Divisional ☐ Continuation-in-part (CIP) of prior application No.: \_\_\_\_\_

Which is a:

☐ Continuation ☐ Divisional ☐ Continuation-in-part (CIP) of prior application No.: \_\_\_\_\_

Which is a:

☐ Continuation ☐ Divisional ☐ Continuation-in-part (CIP) of prior application No.: \_\_\_\_\_

Enclosed are:

**Application Elements**

1. ☐ Filing fee as calculated and transmitted as described below
2. ☒ Specification having 40 pages and including the following:
  - a. ☒ Descriptive Title of the Invention
  - b. ☒ Cross References to Related Applications (if applicable)
  - c. ☐ Statement Regarding Federally-sponsored Research/Development (if applicable)
  - d. ☐ Reference to Microfiche Appendix (if applicable)
  - e. ☒ Background of the Invention
  - f. ☒ Brief Summary of the Invention
  - g. ☒ Brief Description of the Drawings (if drawings filed)
  - h. ☒ Detailed Description
  - i. ☒ Claim(s) as Classified Below
  - j. ☒ Abstract of the Disclosure

# UTILITY PATENT APPLICATION TRANSMITTAL (Large Entity)

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Docket No.  
2204/A55

Total Pages in this Submission  
57

## Application Elements (Continued)

7c918 U.S. PTO  
09/660370  
09/12/00

3. ☒ Drawing(s) (when necessary as prescribed by 35 USC 113)
- a. ☐ Formal Number of Sheets \_\_\_\_\_
- b. ☒ Informal Number of Sheets 9
4. ☒ Oath or Declaration
- a. ☐ Newly executed (original or copy) ☒ Unexecuted
- b. ☐ Copy from a prior application (37 CFR 1.63(d)) (for continuation/divisional application only)
- c. ☒ With Power of Attorney ☐ Without Power of Attorney
- d. ☐ DELETION OF INVENTOR(S)  
Signed statement attached deleting inventor(s) named in the prior application,  
see 37 C.F.R. 1.63(d)(2) and 1.33(b).
5. ☐ Incorporation By Reference (usable if Box 4b is checked)  
The entire disclosure of the prior application, from which a copy of the oath or declaration is supplied under  
Box 4b, is considered as being part of the disclosure of the accompanying application and is hereby  
incorporated by reference therein.
6. ☐ Computer Program in Microfiche (Appendix)
7. ☐ Nucleotide and/or Amino Acid Sequence Submission (if applicable, all must be included)
- a. ☐ Paper Copy
- b. ☐ Computer Readable Copy (identical to computer copy)
- c. ☐ Statement Verifying Identical Paper and Computer Readable Copy

## Accompanying Application Parts

8. ☐ Assignment Papers (cover sheet & document(s))
9. ☐ 37 CFR 3.73(B) Statement (when there is an assignee)
10. ☐ English Translation Document (if applicable)
11. ☐ Information Disclosure Statement/PTO-1449 ☐ Copies of IDS Citations
12. ☐ Preliminary Amendment
13. ☒ Acknowledgment postcard
14. ☒ Certificate of Mailing
- ☐ First Class ☒ Express Mail (Specify Label No.): EL543499998US

SCANNED, #24

# UTILITY PATENT APPLICATION TRANSMITTAL (Large Entity)

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Docket No.  
2204/A55

Total Pages in this Submission  
57

## Accompanying Application Parts (Continued)

15. ☐ Certified Copy of Priority Document(s) (if foreign priority is claimed)
16. ☐ Additional Enclosures (please identify below):

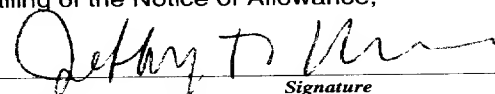
09/12/00  
09/660370  
U.S. PTO

## Fee Calculation and Transmittal

### CLAIMS AS FILED

For	#Filed	#Allowed	#Extra	Rate	Fee
Total Claims	69	- 20 =	49	x \$18.00	\$882.00
Indep. Claims	18	- 3 =	15	x \$78.00	\$1,170.00
Multiple Dependent Claims (check if applicable) <input type="checkbox"/>					\$0.00
BASIC FEE					\$690.00
OTHER FEE (specify purpose)					\$0.00
TOTAL FILING FEE					\$2,742.00

- ☐ A check in the amount of \_\_\_\_\_ to cover the filing fee is enclosed.
- ☐ The Commissioner is hereby authorized to charge and credit Deposit Account No. \_\_\_\_\_ as described below. A duplicate copy of this sheet is enclosed.
- ☐ Charge the amount of \_\_\_\_\_ as filing fee.
- ☐ Credit any overpayment.
- ☐ Charge any additional filing fees required under 37 C.F.R. 1.16 and 1.17.
- ☐ Charge the issue fee set in 37 C.F.R. 1.18 at the mailing of the Notice of Allowance, pursuant to 37 C.F.R. 1.311(b).

  
Signature

Jeffrey T. Klayman, Reg. No. 39,250  
BROMBERG & SUNSTEIN LLP  
125 Summer Street  
Boston, MA 02110  
(617) 443-9292

Dated: September 12, 2000

CC:

**CERTIFICATE OF MAILING BY "EXPRESS MAIL" (37 CFR 1.10)**Applicant(s): **Hardjono**

Docket No.

2204/A55

Serial No.  
Not Yet AssignedFiling Date  
HerewithExaminer  
Not Yet AssignedGroup Art Unit  
Not Yet AssignedInvention: **SYSTEM, DEVICE, AND METHOD FOR CONTROLLING ACCESS IN A MULTICAST COMMUNICATION NETWORK**I hereby certify that this Utility Patent Application Transmittal and enclosures referred to therein  
(Identify type of correspondence)is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under  
37 CFR 1.10 in an envelope addressed to: The Assistant Commissioner for Patents, Washington, D.C. 20231 on  
September 12, 2000  
(Date)Jeffrey T. Klayman

(Typed or Printed Name of Person Mailing Correspondence)

(Signature of Person Mailing Correspondence)

EL543499998US

("Express Mail" Mailing Label Number)

Note: Each paper must have its own certificate of mailing.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION FOR UNITED STATES PATENT

FOR

**SYSTEM, DEVICE, AND METHOD FOR CONTROLLING ACCESS  
IN A MULTICAST COMMUNICATION NETWORK**

Inventor:

**Thomas P. Hardjono**  
430 Highland Avenue  
Winchester, MA 01890

Attorney Docket No.: 2204/A55

Client Reference No.: BA0472

Attorneys:

**BROMBERG & SUNSTEIN LLP**  
125 Summer Street  
Boston, MA 02110  
(617) 443-9292

## **SYSTEM, DEVICE, AND METHOD FOR CONTROLLING ACCESS IN A MULTICAST COMMUNICATION NETWORK**

5

### **PRIORITY**

10

The present patent application claims priority from the commonly-owned United States Provisional Patent Application No. 60/204,218 entitled SYSTEM, DEVICE, AND METHOD FOR CONTROLLING ACCESS IN A MULTICAST COMMUNICATION NETWORK, which was filed on May 15, 2000 in the name of Thomas P. Hardjono, and is hereby incorporated herein by reference in its entirety.

15

### **FIELD OF THE INVENTION**

20

The present invention relates generally to communication systems, and more particularly to controlling access to a shared multicast distribution tree in a Protocol Independent Multicast (PIM) communication network.

25

### **BACKGROUND OF THE INVENTION**

In today's information age, communication networks are often used for transporting information from an information provider to one or more information consumers.

30

One technique for transporting information from an information provider to a group of information consumers over the communication network is known as "multicasting." Multicasting allows the information provider (referred to hereinafter as a "multicast source") to transmit a single unit of multicast information (referred to hereinafter as a "multicast packet") simultaneously to all information consumers (referred to hereinafter individually as a "multicast client" and collectively as "multicast clients") in the multicast group, specifically by addressing the multicast packet to the multicast group using a multicast address. The multicast clients monitor the communication network for multicast packets addressed to the multicast group.

In order to distribute multicast packets from a particular multicast source S to the multicast clients for a particular multicast group G, the multicast packet is routed through the communication network by a number of routers. The communication network may include multiple routing domains, and therefore the multicast packet may traverse multiple routing domains. Each router runs various routing protocols to determine, among other things, a "next hop" for each packet based upon address information in the packets. Such routing information is used to establish a multicast distribution tree (referred to hereinafter as the "shared tree"), and is maintained by each router in one or more routing tables (often referred to as a "routing information base").

One problem that plagues many multicast communication networks is security, or more specifically, the lack thereof. Many multicast communication networks are based upon an anonymous receiver model in which any host can join the shared tree, for example, using a group management mechanism such as the Internet Group Management Protocol (IGMP) as described in Fenner, Internet Engineering Task Force (IETF) Request for Comments (RFC) 2236, Internet Group Management Protocol, Version 2 (November 1997), which is hereby incorporated herein by reference in its entirety. This anonymous receiver model exposes the shared tree to various types of attacks.

One attempt to protect the shared tree involves the use of data encryption to prevent unauthorized hosts from accessing multicast data. For data encryption, a group-wide encryption key (referred to hereinafter as the "group key") is used to encrypt and decrypt all multicast data for a particular multicast group. The group key is distributed to the multicast source as well as to all authorized multicast clients (hosts). The multicast source uses the group key to encrypt the multicast data, while all authorized multicast clients use the group key to decrypt the multicast data. Unauthorized hosts that receive the encrypted multicast data are unable to decrypt the multicast data, and are therefore prevented from accessing the multicast data.

Another attempt to protect the shared tree involves the authentication of control messages between multicast routers. Specifically, the multicast routers exchange various control messages for, among other things, joining the shared tree. These control messages are authenticated hop-by-hop according to a predetermined authentication scheme. By

-3-

authenticating all control messages, only authorized multicast routers are able to join the shared tree.

Unfortunately, neither data encryption nor control message authentication prevents an unauthorized host from joining the shared tree and thereby consuming valuable communication resources. Because authentication operates only between the multicast routers, an unauthorized host can still join the shared tree, specifically by sending a join request, for example, using IGMP or other group management mechanism. The multicast routers establish the appropriate multicast routes for routing multicast packets to the unauthorized host, perhaps even using authentication to perform hop-by-hop authentication. As a member of the shared tree, the unauthorized host receives multicast packets. This is true even if the multicast packets are protected using data encryption, in which case the unauthorized host simply discards the encrypted multicast data.

Thus, a technique for controlling access in a multicast communication network is needed.

### SUMMARY OF THE INVENTION

An unauthorized host device is prevented from joining the PIM shared tree using a centralized host authentication mechanism. Each authorized host is allocated a unique authentication key, which is used by the designated router to encode the PIM join message and by the rendezvous point router to authenticate the PIM join message. If the PIM join message is authentic, then each PIM router from the rendezvous point router to the designated router establishes appropriate multicast routes to route multicast packets to the host. If the PIM join message is not authentic, then multicast packets are prevented from reaching the host. Otherwise, the host device is added to the shared tree and receives multicast packets forwarded by the rendezvous point router.

### BRIEF DESCRIPTION OF THE DRAWINGS



The foregoing and other objects and advantages of the invention will be appreciated more fully from the following further description thereof with reference to the accompanying drawings wherein:

FIG. 1 is a network diagram showing an exemplary PIM communication network in accordance with an embodiment of the present invention;

FIG. 2 is a logic flow diagram showing exemplary key server logic in accordance with an embodiment of the present invention;

FIG. 3 is a logic flow diagram showing exemplary host logic in accordance with an embodiment of the present invention;

FIG. 4 is a logic flow diagram showing exemplary designated router (DR) logic in accordance with an embodiment of the present invention;

FIG. 5 is a logic flow diagram showing exemplary intermediate PIM router logic in accordance with an embodiment of the present invention in which the intermediate PIM router is not already joined to the shared tree;

FIG. 6 is a logic flow diagram showing exemplary intermediate PIM router logic in accordance with an embodiment of the present invention in which the intermediate PIM router is already joined to the shared tree;

FIG. 7 is a logic flow diagram showing exemplary rendezvous point (RP) logic in accordance with an embodiment of the present invention;

FIG. 8 is a communication message diagram showing the relevant fields of an exemplary GKM protocol message in accordance with an embodiment of the present invention;

FIG. 9 is a communication message diagram showing the relevant fields of an exemplary tagged PIM join message in accordance with an embodiment of the present invention;

FIG. 10 is a communication message diagram showing the relevant fields of an exemplary explicit acknowledgment in accordance with an embodiment of the present invention; and

FIG. 11 is a communication message diagram showing the relevant fields of an exemplary extended IGMP join request message in accordance with an embodiment of the present invention.

## DETAILED DESCRIPTION OF A PREFERRED EMBODIMENT

An embodiment of the present invention uses a centralized host authentication scheme to prevent unauthorized hosts from joining the shared tree. This centralized host authentication scheme is in addition to data encryption and control message authentication.

In the centralized host authentication scheme of an embodiment of the present invention, host authentication is performed by a central device when the host attempts to join the shared tree. Specifically, an authorized host obtains an authentication key, for example, from a key server. The authentication key is also sent to the central device, for example, by the key server, and to an access device through which the host accesses the shared tree, for example, by the host within an IGMP join request. In any case, upon receiving an IGMP join request from the host, the access device generates an encoded join request using the authentication key for the host, and forwards the encoded join request upstream toward the central device. Upon receiving the encoded join request, the central device authenticates the encoded join request using the authentication key for the host. If the encoded join message is authentic, then each intermediate device from the central device to the access device establishes appropriate multicast routes to route multicast packets to the host. If the encoded join message is not authentic, then multicast packets are prevented from reaching the host.

Various aspects of the present invention are described herein with reference to a Protocol Independent Multicast (PIM) communication network. PIM is a well-known protocol for routing multicast packets within a multicast routing domain. PIM is so named because it is not dependent upon any particular unicast routing protocol for setting up a multicast distribution tree within the multicast routing domain. PIM has two modes of operation, specifically a sparse mode and a dense mode. PIM Sparse Mode (PIM-SM) is described in Estrin et al., Internet Engineering Task Force (IETF) Request For Comments

(RFC) 2362, Protocol Independent Multicast - Sparse Mode (PIM-SM): Protocol Specification (June 1998), which is hereby incorporated herein by reference in its entirety. PIM Dense Mode (PIM-DM) is described in Deering et al., Internet Engineering Task Force (IETF) Internet Draft draft-ietf-pim-v2-dm-03.txt, Protocol Independent Multicast Version 2 Dense Mode Specification (June 7, 1999), which is hereby incorporated herein by reference in its entirety.

In accordance with the PIM protocol, the various routers within a particular PIM domain establish a default multicast distribution tree, referred to as a "shared tree," for each multicast group. Each shared tree is rooted at a Rendezvous Point (RP) router (i.e., the central device) that acts as the distribution point of all multicast packets for the multicast group. Before a router can join the shared tree for a particular multicast group, the router must learn the identity of the multicast group RP router. A router learns the identity of the multicast group RP router by receiving a PIM Bootstrap Message including a list of all RP routers in the PIM domain. The router receives the PIM Bootstrap Message either from a Bootstrap Router (BSR), which sends the PIM Bootstrap Message to all routers in the PIM domain at predetermined intervals (typically every 60 seconds), or from a neighboring router, which sends the PIM Bootstrap Message to the router if and only if the neighboring router has lost contact with the router for a predetermined period of time (typically 105 seconds). Upon learning the identity of the multicast group RP router, or at any time thereafter, each router that supports a downstream multicast group member (i.e., multicast client) joins the shared tree by sending a PIM Join/Prune Message hop-by-hop toward the multicast group RP router. Each intermediate router that receives the PIM Join/Prune Message from a downstream router also joins the shared tree by forwarding the PIM Join/Prune Message toward the multicast group RP router.

Typically, a PIM router joins the shared tree when a downstream multicast client joins the shared tree. Specifically, each host accesses the shared tree through a PIM router that is referred to as the Designated Router (DR) for that host (i.e., the access device). The host and the DR support a multicast group management protocol, such as IGMP. In order to join the shared tree, the host sends a join request to the DR using the multicast group management protocol, and the DR forwards a PIM join message upstream towards the RP.

-7-

Each PIM router that receives the PIM join message establishes the appropriate multicast routes for routing multicast packets to the host, and also joins the shared tree (if it is not already joined to the shared tree) by forwarding the PIM join message upstream towards the RP.

5           Data encryption may be used to prevent unauthorized hosts from accessing multicast data. For data encryption, a group-wide encryption key (referred to hereinafter as the “group key”) is used to encrypt and decrypt all multicast data for a particular multicast group. The group key is distributed to the multicast source as well as to all authorized multicast clients (hosts). The multicast source uses the group key to encrypt the multicast data, while all authorized multicast clients use the group key to decrypt the multicast data. Unauthorized hosts that receive the encrypted multicast data are unable to decrypt the multicast data, and are therefore prevented from accessing the multicast data.

10           Authentication may be used to prevent unauthorized routers from joining the PIM shared tree. For PIM authentication, all PIM control messages are authenticated hop-by-hop from the DR to the RP, as described in Wei, Internet Engineering Task Force (IETF) Internet Draft draft-ietf-pim-v2-auth-00.txt, Authenticating PIM Version 2 Messages (November 11, 1998), which is hereby incorporated herein by reference in its entirety. PIM authentication is performed using IPsec AH and a symmetric encryption key that is shared by all routers in the PIM domain (referred to hereinafter as the “equal-opportunity key”), as described in Kent et al., Internet Engineering Task Force (IETF) Request for Comments (RFC) 2401, Security Architecture for the Internet Protocol (November 1998), which is hereby incorporated herein by reference in its entirety. By authenticating all PIM control messages, only authorized PIM routers are able to join the shared tree.

15           FIG. 1 shows an exemplary PIM communication network 100. The exemplary PIM communication network 100 includes key server (118), BSR (120), RP (106), intermediate PIM router (108), multicast source S (102), two multicast hosts H1 (112) and H2 (116), and three designated routers DR (104), DR1 (110), and DR2 (114). The multicast source S (102) accesses the shared tree via DR (104). The multicast host H1 (112) accesses the shared tree via DR1 (110). The multicast host H2 (116) accesses the

shared tree via DR2 (114). The three designated routers DR (104), DR1 (110), and DR2 (114) are coupled through RP (106) and the intermediate PIM router (108).

In an exemplary embodiment of the present invention, an authorized host is allocated a unique authentication key (referred to hereinafter as the "DR key"). The DR key is distributed to the DR, for example, by the host within an IGMP join request. The DR key is used by the DR to encode a corresponding PIM join message and by the RP to authenticate the PIM join message. If the PIM join message is authentic, then each PIM router from the RP to the DR establishes appropriate multicast routes to route multicast packets to the host. If the PIM join message is not authentic, then multicast packets are prevented from reaching the host.

The DR key is distributed to the host using a key distribution protocol that is typically scalable, secure, and independent of the underlying unicast and multicast routing protocols. Because the host already uses a group key management (GKM) protocol to obtain a group key for data encryption from a secure key server, it is preferable for the host to also use the GKM protocol to obtain the DR key from the key server. Specifically, the host uses the GKM protocol to request the group key from the key server. Upon receiving the request from the host using the GKM protocol, the key server authenticates the host and, assuming the host is authorized to receive the group key, generates a unique DR key for the host and sends both the group key and the DR key to the host using the GKM protocol.

FIG. 2 shows exemplary key server logic 200. Beginning at block 202, and upon receiving a request from the host, the logic authenticates the host, in block 204, to determine whether the host is authorized to receive the group key. Assuming the host is authorized to receive the group key, the logic allocates a unique DR key for the host, in block 206. The logic then forwards both the group key and the DR key to the host, in block 208, for example, using the GKM protocol. The logic also forwards the DR key to the RP, in block 210. The logic 200 terminates at block 299.

FIG. 8 shows the relevant fields of an exemplary GKM protocol message 800. The GKM protocol message 800 includes, among other things, a group key field 802 and a DR

key field 804. The GKM protocol message 800 is sent by the key server 118 to the host as part of the group key management function.

After receiving its DR key from the key server using the GKM protocol, the host sends its DR key to its DR. The host may send the DR key to the DR prior to sending a join request to the DR, although the host preferably includes the DR key in the join request, for example, in an extended IGMP join request that includes a DR key field.

FIG. 3 shows exemplary host logic 300. Beginning at block 302, and upon obtaining the DR key from the key server 118, the logic sends the DR key to the DR 104, in block 306, and sends a join request to the DR 104, in block 308. In a typical embodiment of the invention, the host sends both the DR key and the join request in an extended IGMP join request that includes a DR key field. The logic 300 terminates at block 399.

FIG. 11 shows the relevant fields of an exemplary extended IGMP join request message 1100. The extended IGMP join request message 1100 includes, among other things, a join field 1102 and a DR key field 1104. The extended IGMP join request message 1100 is sent by the host to the DR in order to join the shared tree. The host includes its DR key in the DR field 1104.

In any case, after receiving both the DR key and the join request, the DR generates a specially formatted PIM join message that can be authenticated using the DR key. In an exemplary embodiment of the invention, the specially formatted PIM join message includes, among other things, a (join, tag, nonce) triplet that is treated as a payload to be protected using PIM authentication, and is referred to hereinafter as a “tagged” PIM join message. The tag is preferably a digest/MAC that the DR computes using a keyed hash function and the DR key. The nonce is a number that the DR changes each time it generates a tagged PIM join message, and is used in part to prevent a “playback” attack. The DR forwards the tagged PIM join message (with PIM authentication) upstream toward the RP.

FIG. 4 shows exemplary DR logic 400. Beginning at block 402, and upon receiving the DR key from the host, in block 404, as well as a join request from the host, in block 406, the logic generates a tag using the DR key, in block 408. The logic also

generates a nonce, in block 410. The logic generates a tagged PIM join message including, among other things, the tag and the nonce, in block 412. Assuming PIM Authentication is used, the logic encrypts the tagged PIM join message using the equal opportunity key according to IPsec AH, in block 414, and forwards the tagged PIM join message upstream toward the RP 106, in block 416. The logic 400 terminates at block 499.

FIG. 9 shows the relevant fields of an exemplary tagged PIM join message 900. The tagged PIM join message 900 includes, among other things, a join field 902, a tag field 904, and a nonce field 906. The tagged PIM join message is generated by the DR and forwarded by the DR upstream toward the RP 106.

Each intermediate PIM router between the DR and the RP processes the tagged PIM join message and forwards the tagged PIM join message upstream toward the RP. Specifically, after authenticating the tagged PIM join message using the equal opportunity key, the intermediate PIM router determines whether or not it is already joined to the shared tree.

If the intermediate PIM router is not already joined to the shared tree, then the intermediate PIM router is not yet receiving multicast packets. Therefore, the intermediate PIM router establishes multicast routes for forwarding multicast packets to the host, and forwards the tagged PIM join message upstream toward the RP. If the host is authentic, then the intermediate PIM router will receive multicast packets from its upstream neighbor for forwarding to the host. If the host is not authentic, then the intermediate PIM router will not receive multicast packets from its upstream neighbor, and the intermediate PIM router will eventually remove the multicast routes.

However, if the intermediate PIM router is already joined to the shared tree, then the intermediate PIM router is already receiving and forwarding multicast packets, and cannot simply establish multicast routes for forwarding multicast packets to the host. This is because, by establishing such multicast routes, multicast packets would be forwarded to the host even if the host ultimately fails authentication. Therefore, before establishing such multicast routes, the intermediate PIM router forwards the tagged PIM join message upstream toward the RP and waits for an explicit acknowledgment from the RP indicating

-11-

that the host is authentic. The intermediate PIM router preferably also saves a copy of the tagged PIM join message for correlation to the explicit acknowledgment.

As discussed below with reference to the RP, the intermediate PIM router may or may not receive the explicit acknowledgment (or may receive an explicit negative acknowledgment indicating that the host is not authentic). If the intermediate PIM router receives the explicit acknowledgment from the RP indicating that the host is authentic, then the intermediate PIM router establishes multicast routes for forwarding multicast packets to the host. If the intermediate PIM router does not receive the explicit acknowledgment from the RP indicating that the host is authentic (or receives the explicit negative acknowledgment), then the intermediate PIM router does not establish multicast routes for forwarding multicast packets to the host.

FIGs. 5 and 6 show exemplary intermediate PIM router logic 500 for processing the tagged PIM join message. Beginning at block 502, and upon receiving the tagged PIM join message, in block 504, the logic authenticates the tagged PIM join message using the equal opportunity key according to IPsec AH, in block 506. If the tagged PIM join message is not authentic (NO in block 508), then the logic 500 terminates at block 599. If the tagged PIM join message is authentic (YES in block 508), then the logic determines whether the router is already joined to the shared tree, in block 510. If the router is not already joined to the shared tree (NO in block 512), then the logic proceeds to block 514. If the router is already joined to the shared tree (YES in block 512), then the logic proceeds to block 600.

At block 514, the logic establishes appropriate multicast routes for forwarding multicast packets downstream toward the host. The logic also forwards the tagged PIM join message upstream toward the RP 106, in block 516. The logic 500 terminates at block 599.

At block 600, as shown in FIG. 6, the logic stores a copy of the tagged PIM join message, in block 602, and forwards the tagged PIM join message upstream toward the RP 106, in block 604. The logic waits for an explicit acknowledgment from the RP 106, in block 606. Upon receiving the explicit acknowledgment from the RP 106, in block 608, the logic compares the explicit acknowledgment to the stored copy of the tagged PIM join



-12-

message, in block 610, specifically to verify that the explicit acknowledgment corresponds to the tagged PIM join message. Upon determining that the explicit acknowledgment corresponds to the tagged PIM join message, in block 612, the logic establishes appropriate multicast routes for forwarding multicast packets downstream toward the host, in block 614. The logic 500 terminates at block 599.

Eventually, the RP router receives the tagged PIM join message that was generated by the DR and forwarded upstream by the intermediate PIM routers. The RP maintains a list of all DR keys, which it obtains from the key server over a secure communication link. Upon receiving the tagged PIM join message, the RP searches the list of DR keys for the DR key associated with the host, and uses the DR key to authenticate the tagged PIM join message. Specifically, the RP uses the DR key to verify the tag using the keyed hash function. If the RP determines that the tagged PIM join message is authentic, then the RP generates an explicit acknowledgment including both the tag and the nonce and forwards the explicit acknowledgment downstream toward the host. If the RP fails to find the DR key associated with the host or the RP determines that the tagged PIM join message is not authentic, then the RP considers the host to be unauthorized, in which case the RP does not generate an explicit acknowledgment (or alternatively generates an explicit negative acknowledgment).

FIG. 7 shows exemplary RP logic 700. Beginning at block 702, and upon receiving the tagged PIM join message, in block 704, the logic authenticates the tagged PIM join message using the equal opportunity key according to IPsec AH, in block 706. If the tagged PIM join message is not authentic (NO in block 707), then the logic 700 terminates at block 799. If the tagged PIM join message is authentic (YES in block 707), then the logic searches for the DR key associated with the host, in block 708, specifically from a list of DR keys maintained by the RP. If the RP fails to find the DR key associated with the host (NO in block 710), then the logic 700 terminates at block 799. If the RP finds the DR key associated with the host (YES in block 710), then the logic authenticates the tagged PIM join message using the DR key associated with the host, in block 712. If the tagged PIM join message is not authentic (NO in block 714), then the logic 700 terminates at block 799. If the tagged PIM join message is authentic (YES in block 714),

-13-

then the logic establishes appropriate multicast routes for forwarding multicast packets to the host, in block 716, and sends an explicit acknowledgment downstream toward the host, in block 718. The logic 700 terminates at block 799.

FIG. 10 shows the relevant fields of an exemplary explicit acknowledgment 1000.

5 The explicit acknowledgment 1000 includes, among other things, an acknowledgement (ACK) field 1002, a tag field 1004, and a nonce field 1006. The RP generates the explicit acknowledgment 1000 and forwards it downstream toward the host. The RP sets the tag field 1004 and the nonce field 1006 equal to the tag field 904 and nonce field 906, respectively, from the tagged PIM join message so that the intermediate PIM routers can correlate the explicit acknowledgment to the tagged PIM join message.

10 It should be noted that the term "router" is used herein to describe a communication device that may be used in a communication system, and should not be construed to limit the present invention to any particular communication device type. Thus, a communication device may include, without limitation, a bridge, router, bridge-router (brouter), switch, node, or other communication device.

15 It should also be noted that the term "packet" is used herein to describe a communication message that may be used by a communication device (*e.g.*, created, transmitted, received, stored, or processed by the communication device) or conveyed by a communication medium, and should not be construed to limit the present invention to any particular communication message type, communication message format, or communication protocol. Thus, a communication message may include, without limitation, a frame, packet, datagram, user datagram, cell, or other type of communication message.

20 It should also be noted that the logic flow diagrams are used herein to demonstrate various aspects of the invention, and should not be construed to limit the present invention to any particular logic flow or logic implementation. The described logic may be partitioned into different logic blocks (*e.g.*, programs, modules, functions, or subroutines) without changing the overall results or otherwise departing from the true scope of the invention. Often times, logic elements may be added, modified, omitted, performed in a different order, or implemented using different logic constructs (*e.g.*, logic gates, looping

25

30

primitives, conditional logic, and other logic constructs) without changing the overall results or otherwise departing from the true scope of the invention.

The present invention may be embodied in many different forms, including, but in no way limited to, computer program logic for use with a processor (*e.g.*, a microprocessor, microcontroller, digital signal processor, or general purpose computer), programmable logic for use with a programmable logic device (*e.g.*, a Field Programmable Gate Array (FPGA) or other PLD), discrete components, integrated circuitry (*e.g.*, an Application Specific Integrated Circuit (ASIC)), or any other means including any combination thereof. In a typical embodiment of the present invention, predominantly all of the described logic is implemented as a set of computer program instructions that is converted into a computer executable form, stored as such in a computer readable medium, and executed by a microprocessor within the corresponding communication device (host, key server, DR, intermediate PIM router, RP) under the control of an operating system.

Computer program logic implementing all or part of the functionality previously described herein may be embodied in various forms, including, but in no way limited to, a source code form, a computer executable form, and various intermediate forms (*e.g.*, forms generated by an assembler, compiler, linker, or locator). Source code may include a series of computer program instructions implemented in any of various programming languages (*e.g.*, an object code, an assembly language, or a high-level language such as Fortran, C, C++, JAVA, or HTML) for use with various operating systems or operating environments. The source code may define and use various data structures and communication messages. The source code may be in a computer executable form (*e.g.*, via an interpreter), or the source code may be converted (*e.g.*, via a translator, assembler, or compiler) into a computer executable form.

The computer program may be fixed in any form (*e.g.*, source code form, computer executable form, or an intermediate form) either permanently or transitorily in a tangible storage medium, such as a semiconductor memory device (*e.g.*, a RAM, ROM, PROM, EEPROM, or Flash-Programmable RAM), a magnetic memory device (*e.g.*, a diskette or fixed disk), an optical memory device (*e.g.*, a CD-ROM), or other memory device. The computer program may be fixed in any form in a signal that is transmittable to a computer

-15-

using any of various communication technologies, including, but in no way limited to, analog technologies, digital technologies, optical technologies, wireless technologies, networking technologies, and internetworking technologies. The computer program may be distributed in any form as a removable storage medium with accompanying printed or electronic documentation (*e.g.*, shrink wrapped software), preloaded with a computer system (*e.g.*, on system ROM or fixed disk), or distributed from a server or electronic bulletin board over the communication system (*e.g.*, the Internet or World Wide Web).

Hardware logic (including programmable logic for use with a programmable logic device) implementing all or part of the functionality previously described herein may be designed using traditional manual methods, or may be designed, captured, simulated, or documented electronically using various tools, such as Computer Aided Design (CAD), a hardware description language (*e.g.*, VHDL or AHDL), or a PLD programming language (*e.g.*, PALASM, ABEL, or CUPL).

Programmable logic may be fixed either permanently or transitorily in a tangible storage medium, such as a semiconductor memory device (*e.g.*, a RAM, ROM, PROM, EEPROM, or Flash-Programmable RAM), a magnetic memory device (*e.g.*, a diskette or fixed disk), an optical memory device (*e.g.*, a CD-ROM), or other memory device. The programmable logic may be fixed in a signal that is transmittable to a computer using any of various communication technologies, including, but in no way limited to, analog technologies, digital technologies, optical technologies, wireless technologies, networking technologies, and internetworking technologies. The programmable logic may be distributed as a removable storage medium with accompanying printed or electronic documentation (*e.g.*, shrink wrapped software), preloaded with a computer system (*e.g.*, on system ROM or fixed disk), or distributed from a server or electronic bulletin board over the communication system (*e.g.*, the Internet or World Wide Web).

Thus, the present invention may be embodied as a communication system having a rendezvous point device that forwards multicast communication messages to members of a shared tree, a designated device in communication with the rendezvous point device via a number of intermediate devices, and a host device in communication with the designated device. The host device sends a join request to the designated device using a

-16-

predetermined multicast group management protocol in order to join the shared tree for receiving the multicast communication messages forwarded by the rendezvous point device. The designated device receives the join request and forwards to the rendezvous point device via the number of intermediate devices an encoded join request generated using an authentication key associated with the host device. The rendezvous point device receives the encoded join request and authenticates the encoded join message using the authentication key associated with the host device. The host device is prevented from receiving the multicast communication messages forwarded by the rendezvous point device if the rendezvous point device determines that the encoded join request is not authentic, but is added to the shared tree if the rendezvous point device determines that the encoded join request is authentic. In the communication system, a key server may authenticate the host device, generate the authentication key for the host device, and provide the authentication key to both the host device and the rendezvous point device using a secure key distribution mechanism. The designated device obtains the authentication key, preferably from the host device included within the join request.

The present invention may also be embodied as key server logic for authenticating a host device, generating an authentication key for the host device, and sending the authentication key to the host device and to a rendezvous point device using a secure key distribution mechanism.

The present invention may also be embodied as host device logic for obtaining an authentication key and sending a join request to a designated device using a predetermined multicast group management protocol. The join request includes the authentication key. The predetermined multicast group management protocol is preferably an extended Internet Group Management Protocol (IGMP) including means for including the authentication key in the join request.

The present invention may also be embodied as DR logic for receiving a join request from a host device, generating an encoded join request using an authentication key associated with the host device, and sending the encoded join request toward a rendezvous point device. The join request preferably includes the authentication key. The DR also

-17-

joins a shared tree on behalf of the host device and establishes appropriate multicast routes for forwarding multicast communication messages to the host device.

The present invention may also be embodied as intermediate device logic for receiving an encoded join request for a host device and forwarding the encoded join request toward a rendezvous point device. The intermediate device may join a shared tree and establish appropriate multicast routes for forwarding multicast communication messages toward the host device, if the intermediate device is not already joined to the shared tree, or else the intermediate device may wait for an explicit acknowledgment message from the rendezvous point device before establishing appropriate multicast routes for forwarding multicast communication messages toward the host device, if the intermediate device is already joined to the shared tree.

The present invention may also be embodied as rendezvous point device logic for receiving an encoded join request for a host device, authenticating the encoded join request to determine whether or not the encoded join request is authentic, and establishing appropriate multicast routes for forwarding multicast communication messages to the host device if and only if the encoded join request is determined to be authentic. Authenticating the encoded join request involves maintaining a number of authentication keys, determining the host device for the encoded join request, and searching for an authentication key associated with the host device. If there is no authentication key associated with the host device, then the encoded join request is considered to be not authentic. If there is an authentication key associated with the host device, then the authentication key is used to authenticate the encoded join request. The rendezvous point device may send an explicit acknowledgment if the encoded join request is determined to be authentic.

The present invention may also be embodied as a method in a communication system having a host device, a designated device, and a rendezvous point device. The method involves sending a join request by the host device to the designated device in order to join a shared tree, sending an encoded join request by the designated device to the rendezvous point device, authenticating the encoded join request by the rendezvous point device, adding the host device to the shared tree if the encoded join request is authentic,

-18-

and excluding the host device from the shared tree if the encoded join request is not authentic.

The present invention may also be embodied as a communication message embodied in a data signal. The communication message may be a key distribution message including a group key for a multicast group and an authentication key for a host device. The communication message may be a join request including an authentication key for a host device. The communication message may be an encoded join request including a tag field and a nonce field. The communication message may be an explicit acknowledgment including a tag field and a nonce field.

The present invention may be embodied in other specific forms without departing from the true scope of the invention. The described embodiments are to be considered in all respects only as illustrative and not restrictive.

I claim:

1. A communication system comprising:

a rendezvous point device that forwards multicast communication messages to  
members of a shared tree;

a designated device in communication with the rendezvous point device via a  
number of intermediate devices; and

a host device in communication with the designated device, wherein:

the host device sends a join request to the designated device using a predetermined  
multicast group management protocol in order to join the shared tree for receiving the  
multicast communication messages forwarded by the rendezvous point device;

the designated device receives the join request and forwards to the rendezvous  
point device via the number of intermediate devices an encoded join request generated  
using an authentication key associated with the host device;

the rendezvous point device receives the encoded join request and authenticates the  
encoded join message using the authentication key associated with the host device; and

the host device is prevented from receiving the multicast communication messages  
forwarded by the rendezvous point device, if the rendezvous point device determines that  
the encoded join message is not authentic.

2. The communication system of claim 1, further comprising a key server for  
authenticating the host device and generating the authentication key for the host device.

3. The communication system of claim 2, wherein the key server provides the  
authentication key to both the host device and the rendezvous point device using a secure  
key distribution mechanism.

4. The communication system of claim 1, wherein the host device sends the  
authentication key to the designated device.



-20-

5. The communication system of claim 4, wherein the host device sends the authentication key to the designated device in the join request.

6. The communication system of claim 5, wherein the predetermined multicast group management protocol is an extended Internet Group Management Protocol (IGMP) including means for including the authentication key in the join request.

7. The communication system of claim 1, wherein the designated device joins the shared tree on behalf of the host device.

8. The communication system of claim 7, wherein the designated device establishes appropriate multicast routes for forwarding multicast communication messages to the host.

9. The communication system of claim 1, wherein each intermediate device receives the encoded join request and forwards the encoded join request toward the rendezvous point device.

10. The communication system of claim 9, wherein each intermediate device that is not already joined to the shared tree joins the shared tree on behalf of the host device and establishes appropriate multicast routes for forwarding multicast communication messages toward the host device upon receiving the encoded join request.

11. The communication system of claim 9, wherein each intermediate device that is already joined to the shared tree waits for an explicit acknowledgment message from the rendezvous point device and establishes appropriate multicast routes for forwarding multicast communication messages toward the host device only upon receiving the explicit acknowledgment message from the rendezvous point device.

- 
- Figure 1 displays 12 histograms, labeled  $x_1$  through  $x_{12}$ , showing the distribution of the number of non-zero elements in the vector  $x_k$ . The x-axis represents the number of non-zero elements (0 to 10), and the y-axis represents the count (0 to 10). The distributions are roughly bell-shaped and centered around 5, with the peak count increasing from 10 for  $x_1$  to 12 for  $x_{12}$ .

- using a secure key distribution mechanism.

-23-

14. An apparatus comprising:

authentication logic operably coupled to authenticate a host device;

key generation logic operably coupled to generate an authentication key for the  
host device; and

5 key distribution logic operably coupled to send the authentication key to the host  
device and to a rendezvous point device using a secure key distribution mechanism.

10  
15  
20  
25  
30  
35  
40  
45  
50  
55  
60  
65  
70  
75  
80  
85  
90  
95  
100  
105  
110  
115  
120  
125  
130  
135  
140  
145  
150  
155  
160  
165  
170  
175  
180  
185  
190  
195  
200  
205  
210  
215  
220  
225  
230  
235  
240  
245  
250  
255  
260  
265  
270  
275  
280  
285  
290  
295  
300  
305  
310  
315  
320  
325  
330  
335  
340  
345  
350  
355  
360  
365  
370  
375  
380  
385  
390  
395  
400  
405  
410  
415  
420  
425  
430  
435  
440  
445  
450  
455  
460  
465  
470  
475  
480  
485  
490  
495  
500  
505  
510  
515  
520  
525  
530  
535  
540  
545  
550  
555  
560  
565  
570  
575  
580  
585  
590  
595  
600  
605  
610  
615  
620  
625  
630  
635  
640  
645  
650  
655  
660  
665  
670  
675  
680  
685  
690  
695  
700  
705  
710  
715  
720  
725  
730  
735  
740  
745  
750  
755  
760  
765  
770  
775  
780  
785  
790  
795  
800  
805  
810  
815  
820  
825  
830  
835  
840  
845  
850  
855  
860  
865  
870  
875  
880  
885  
890  
895  
900  
905  
910  
915  
920  
925  
930  
935  
940  
945  
950  
955  
960  
965  
970  
975  
980  
985  
990  
995

-24-

15. A computer readable medium having embodied therein a computer program for controlling a computer system, the computer program comprising:

authentication logic programmed to authenticate a host device;

key generation logic programmed to generate an authentication key for the host device; and

key distribution logic programmed to send the authentication key to the host device and to a rendezvous point device using a secure key distribution mechanism.

16. The computer readable medium of claim 15, wherein the computer readable medium is a computer storage medium.

17. The computer readable medium of claim 15, wherein the computer readable medium is a computer communication medium.

10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59  
60  
61  
62  
63  
64  
65  
66  
67  
68  
69  
70  
71  
72  
73  
74  
75  
76  
77  
78  
79  
80  
81  
82  
83  
84  
85  
86  
87  
88  
89  
90  
91  
92  
93  
94  
95  
96  
97  
98  
99  
100  
101  
102  
103  
104  
105  
106  
107  
108  
109  
110  
111  
112  
113  
114  
115  
116  
117  
118  
119  
120  
121  
122  
123  
124  
125  
126  
127  
128  
129  
130  
131  
132  
133  
134  
135  
136  
137  
138  
139  
140  
141  
142  
143  
144  
145  
146  
147  
148  
149  
150  
151  
152  
153  
154  
155  
156  
157  
158  
159  
160  
161  
162  
163  
164  
165  
166  
167  
168  
169  
170  
171  
172  
173  
174  
175  
176  
177  
178  
179  
180  
181  
182  
183  
184  
185  
186  
187  
188  
189  
190  
191  
192  
193  
194  
195  
196  
197  
198  
199  
200  
201  
202  
203  
204  
205  
206  
207  
208  
209  
210  
211  
212  
213  
214  
215  
216  
217  
218  
219  
220  
221  
222  
223  
224  
225  
226  
227  
228  
229  
230  
231  
232  
233  
234  
235  
236  
237  
238  
239  
240  
241  
242  
243  
244  
245  
246  
247  
248  
249  
250  
251  
252  
253  
254  
255  
256  
257  
258  
259  
260  
261  
262  
263  
264  
265  
266  
267  
268  
269  
270  
271  
272  
273  
274  
275  
276  
277  
278  
279  
280  
281  
282  
283  
284  
285  
286  
287  
288  
289  
290  
291  
292  
293  
294  
295  
296  
297  
298  
299  
300  
301  
302  
303  
304  
305  
306  
307  
308  
309  
310  
311  
312  
313  
314  
315  
316  
317  
318  
319  
320  
321  
322  
323  
324  
325  
326  
327  
328  
329  
330  
331  
332  
333  
334  
335  
336  
337  
338  
339  
340  
341  
342  
343  
344  
345  
346  
347  
348  
349  
350  
351  
352  
353  
354  
355  
356  
357  
358  
359  
360  
361  
362  
363  
364  
365  
366  
367  
368  
369  
370  
371  
372  
373  
374  
375  
376  
377  
378  
379  
380  
381  
382  
383  
384  
385  
386  
387  
388  
389  
390  
391  
392  
393  
394  
395  
396  
397  
398  
399  
400  
401  
402  
403  
404  
405  
406  
407  
408  
409  
410  
411  
412  
413  
414  
415  
416  
417  
418  
419  
420  
421  
422  
423  
424  
425  
426  
427  
428  
429  
430  
431  
432  
433  
434  
435  
436  
437  
438  
439  
440  
441  
442  
443  
444  
445  
446  
447  
448  
449  
450  
451  
452  
453  
454  
455  
456  
457  
458  
459  
460  
461  
462  
463  
464  
465  
466  
467  
468  
469  
470  
471  
472  
473  
474  
475  
476  
477  
478  
479  
480  
481  
482  
483  
484  
485  
486  
487  
488  
489  
490  
491  
492  
493  
494  
495  
496  
497  
498  
499  
500  
501  
502  
503  
504  
505  
506  
507  
508  
509  
510  
511  
512  
513  
514  
515  
516  
517  
518  
519  
520  
521  
522  
523  
524  
525  
526  
527  
528  
529  
530  
531  
532  
533  
534  
535  
536  
537  
538  
539  
540  
541  
542  
543  
544  
545  
546  
547  
548  
549  
550  
551  
552  
553  
554  
555  
556  
557  
558  
559  
560  
561  
562  
563  
564  
565  
566  
567  
568  
569  
570  
571  
572  
573  
574  
575  
576  
577  
578  
579  
580  
581  
582  
583  
584  
585  
586  
587  
588  
589  
590  
591  
592  
593  
594  
595  
596  
597  
598  
599  
600  
601  
602  
603  
604  
605  
606  
607  
608  
609  
610  
611  
612  
613  
614  
615  
616  
617  
618  
619  
620  
621  
622  
623  
624  
625  
626  
627  
628  
629  
630  
631  
632  
633  
634  
635  
636  
637  
638  
639  
640  
641  
642  
643  
644  
645  
646  
647  
648  
649  
650  
651  
652  
653  
654  
655  
656  
657  
658  
659  
660  
661  
662  
663  
664  
665  
666  
667  
668  
669  
670  
671  
672  
673  
674  
675  
676  
677  
678  
679  
680  
681  
682  
683  
684  
685  
686  
687  
688  
689  
690  
691  
692  
693  
694  
695  
696  
697  
698  
699  
700  
701  
702  
703  
704  
705  
706  
707  
708  
709  
710  
711  
712  
713  
714  
715  
716  
717  
718  
719  
720  
721  
722  
723  
724  
725  
726  
727  
728  
729  
730  
731  
732  
733  
734  
735  
736  
737  
738  
739  
740  
741  
742  
743  
744  
745  
746  
747  
748  
749  
750  
751  
752  
753  
754  
755  
756  
757  
758  
759  
760  
761  
762  
763  
764  
765  
766  
767  
768  
769  
770  
771  
772  
773  
774  
775  
776  
777  
778  
779  
780  
781  
782  
783  
784  
785  
786  
787  
788  
789  
790  
791  
792  
793  
794  
795  
796  
797  
798  
799  
800  
801  
802  
803  
804  
805  
806  
807  
808  
809  
810  
811  
812  
813  
814  
815  
816  
817  
818  
819  
820  
821  
822  
823  
824  
825  
826  
827  
828  
829  
830  
831  
832  
833  
834  
835  
836  
837  
838  
839  
840  
841  
842  
843  
844  
845  
846  
847  
848  
849  
850  
851  
852  
853  
854  
855  
856  
857  
858  
859  
860  
861  
862  
863  
864  
865  
866  
867  
868  
869  
870  
871  
872  
873  
874  
875  
876  
877  
878  
879  
880  
881  
882  
883  
884  
885  
886  
887  
888  
889  
890  
891  
892  
893  
894  
895  
896  
897  
898  
899  
900  
901  
902  
903  
904  
905  
906  
907  
908  
909  
910  
911  
912  
913  
914  
915  
916  
917  
918  
919  
920  
921  
922  
923  
924  
925  
926  
927  
928  
929  
930  
931  
932  
933  
934  
935  
936  
937  
938  
939  
940  
941  
942  
943  
944  
945  
946  
947  
948  
949  
950  
951  
952  
953  
954  
955  
956  
957  
958  
959  
960  
961  
962  
963  
964  
965  
966  
967  
968  
969  
970  
971  
972  
973  
974  
975  
976  
977  
978  
979  
980  
981  
982  
983  
984  
985  
986  
987  
988  
989  
990  
991  
992  
993  
994  
995  
996  
997  
998  
999  
1000  
1001  
1002  
1003  
1004  
1005  
1006  
1007  
1008  
1009  
1010  
1011  
1012  
1013  
1014  
1015  
1016  
1017  
1018  
1019  
1020  
1021  
1022  
1023  
1024  
1025  
1026  
1027  
1028  
1029  
1030  
1031  
1032  
1033  
1034  
1035  
1036  
1037  
1038  
1039  
1040  
1041  
1042  
1043  
1044  
1045  
1046  
1047  
1048  
1049  
1050  
1051  
1052  
1053  
1054  
1055  
1056  
1057  
1058  
1059  
1060  
1061  
1062  
1063  
1064  
1065  
1066  
1067  
1068  
1069  
1070  
1071  
1072  
1073  
1074  
1075  
1076  
1077  
1078  
1079  
1080  
1081  
1082  
1083  
1084  
1085  
1086  
1087  
1088  
1089  
1090  
1091  
1092  
1093  
1094  
1095  
1096  
1097  
1098  
1099  
1100  
1101  
1102  
1103  
1104  
1105  
1106  
1107  
1108  
1109  
1110  
1111  
1112  
1113  
1114  
1115  
1116  
1117  
1118  
1119  
1120  
1121  
1122  
1123  
1124  
1125  
1126  
1127  
1128  
1129  
1130  
1131  
1132  
1133  
1134  
1135  
1136  
1137  
1138  
1139  
1140  
1141  
1142  
1143  
1144  
1145  
1146  
1147  
1148  
1149  
1150  
1151  
1152  
1153  
1154  
1155  
1156  
1157  
1158  
1159  
1160  
1161  
1162  
1163  
1164  
1165  
1166  
1167  
1168  
1169  
1170  
1171  
1172  
1173  
1174  
1175  
1176  
1177  
1178  
1179  
1180  
1181  
1182  
1183  
1184  
1185  
1186  
1187  
1188  
1189  
1190  
1191  
1192  
1193  
1194  
1195  
1196  
1197  
1198  
1199  
1200  
1201  
1202  
1203  
1204  
1205  
1206  
1207  
1208  
1209  
1210  
1211  
1212  
1213  
1214  
1215  
1216  
1217  
1218  
1219  
1220  
1221  
1222  
1223  
1224  
1225  
1226  
1227  
1228  
1229  
1230  
1231  
1232  
1233  
1234  
1235  
1236  
1237  
1238  
1239  
1240  
1241  
1242  
1243  
1244  
1245  
1246  
1247  
1248  
1249  
1250  
1251  
1252  
1253  
1254  
1255  
1256  
1257  
1258  
1259  
1260  
1261  
1262  
1263  
1264  
1265  
1266  
1267  
1268  
1269  
1270  
1271  
1272  
1273  
1274  
1275  
1276  
1277  
1278  
1279  
1280  
1281  
1282  
1283  
1284  
1285  
1286  
1287  
1288  
1289  
1290  
1291  
1292  
1293  
1294  
1295  
1296  
1297  
1298  
1299  
1300  
1301  
1302  
1303  
1304  
1305  
1306  
1307  
1308  
1309  
1310  
1311  
1312  
1313  
1314  
1315  
1316  
1317  
1318  
1319  
1320  
1321  
1322  
1323  
1324  
1325  
1326  
1327  
1328  
1329  
1330  
1331  
1332  
1333  
1334  
1335  
1336  
1337  
1338  
1339  
1340  
1341  
1342  
1343  
1344  
1345  
1346  
1347  
1348  
1349  
1350  
1351  
1352  
1353  
1354  
1355  
1356  
1357  
1358  
1359  
1360  
1361  
1362  
1363  
1364  
1365  
1366  
1367  
1368  
1369  
1370  
1371  
1372  
1373  
1374  
1375  
1376  
1377  
1378  
1379  
1380  
1381  
1382  
1383  
1384  
1385  
1386  
1387  
1388  
1389  
1390  
1391  
1392  
1393  
1394  
1395  
1396  
1397  
1398  
1399  
1400  
1401  
1402  
1403  
1404  
1405  
1406  
1407  
1408  
1409  
1410  
1411  
1412  
1413  
1414  
1415  
1416  
1417  
1418  
1419  
1420  
1421  
1422  
1423  
1424  
1425  
1426  
1427  
1428  
1429  
1430  
1431  
1432  
1433  
1434  
1435  
1436  
1437  
1438  
1439  
1440  
1441  
1442  
1443  
1444  
1445  
1446  
1447  
1448  
1449  
1450  
1451  
1452  
1453  
1454  
1455  
1456  
1457  
1458  
1459  
1460  
1461  
1462  
1463  
1464  
1465  
1466  
1467  
1468  
1469  
1470  
1471  
1472  
1473  
1474  
1475  
1476  
1477  
1478  
1479  
1480  
1481  
1482  
1483  
1484  
1485  
1486  
1487  
1488  
1489  
1490  
1491  
1492  
1493  
1494  
1495  
1496  
1497  
1498  
1499  
1500  
1501  
1502  
1503  
1504  
1505  
1506  
1507  
1508  
1509  
1510  
1511  
1512  
1513  
1514  
1515  
1516  
1517  
1518  
1519  
1520  
1521  
1522  
1523  
1524  
1525  
1526  
1527  
1528  
1529  
1530  
1531  
1532  
1533  
1534  
1535  
1536  
1537  
1538  
1539  
1540  
1541  
1542  
1543  
1544  
1545  
1546  
1547  
1548  
1549  
1550  
1551  
1552  
1553  
1554  
1555  
1556  
1557  
1558  
1559  
1560  
1561  
1562  
1563  
1564  
1565  
1566  
1567  
1568  
1569  
1570  
1571  
1572  
1573  
1574  
1575  
1576  
1577  
1578  
1579  
1580  
1581  
1582  
1583  
1584  
1585  
1586  
1587  
1588  
1589  
1590  
1591  
1592  
1593  
1594  
1595  
1596  
1597  
1598  
1599  
1600  
1601  
1602  
1603  
1604  
1605  
1606  
1607  
1608  
1609  
1610  
1611  
1612  
1613  
1614  
1615  
1616  
1617  
1618  
1619  
1620  
1621  
1622  
1623  
1624  
1625  
1626  
1627  
1628  
1629  
1630  
1631  
1632  
1633  
1634  
1635  
1636  
1637  
1638  
1639  
1640  
1641  
1642  
1643  
1644  
1645  
1646  
1647  
1648  
1649  
1650  
1651  
1652  
1653  
1654  
1655  
1656  
1657  
1658  
1659  
1660  
1661  
1662  
1663  
1664  
1665  
1666  
1667  
1668  
1669  
1670  
1671  
1672  
1673  
1674  
1675  
1676  
1677  
1678  
1679  
1680  
1681  
1682  
1683  
1684  
1685  
1686  
1687  
1688  
1689  
1690  
1691  
1692  
1693  
1694  
1695  
1696  
1697  
1698  
1699  
1700  
1701  
1702  
1703  
1704  
1705  
1706  
1707  
1708  
1709  
1710  
1711  
1712  
1713  
1714  
1715  
1716  
1717  
1718  
1719  
1720  
1721  
1722  
1723  
1724  
1725  
1726  
1727  
1728  
1729  
1730  
1731  
1732  
1733  
1734  
1735  
1736  
1737  
1738  
1739  
1740  
1741  
1742  
1743  
1744  
1745  
1746  
1747  
1748  
1749  
1750  
1751  
1752  
1753  
1754  
1755  
1756  
1757  
1758  
1759  
1760  
1761  
1762  
1763  
1764  
1765  
1766  
1767  
1768  
1769  
1770  
1771  
1772  
1773  
1774  
1775  
1776  
1777  
1778  
1779  
1780  
1781  
1782  
1783  
1784  
1785  
1786  
1787  
1788  
1789  
1790  
1791  
1792  
1793  
1794  
1795  
1796  
1797  
1798  
1799  
1800  
1801  
1802  
1803  
1804  
1805  
1806  
1807  
1808  
1809  
1810  
1811  
1812  
1813  
1814  
1815  
1816  
1817  
1818  
1819  
1820  
1821  
1822  
1823  
1824  
1825  
1826  
1827  
1828  
1829  
1830  
1831  
1832  
1833  
1834  
1835  
1836  
1837  
1838  
1839  
1840  
1841  
1842  
1843  
1844  
1845  
1846  
1847  
1848  
1849  
1850  
1851  
1852  
1853  
1854  
1855  
1856  
1857  
1858  
1859  
1860  
1861  
1862  
1863  
1864  
1865  
1866  
1867  
1868  
1869  
1870  
1871  
1872  
1873  
1874  
1875  
1876  
1877  
1878  
1879  
1880  
1881  
1882  
1883  
1884  
1885  
1886  
1887  
1888  
1889  
1890  
1891  
1892  
1893  
1894  
1895  
1896  
1897  
1898  
1899  
1900  
1901  
1902  
1903  
1904  
1905  
1906  
1907  
1908  
1909  
1910  
1911  
1912  
1913  
1914  
1915  
1916  
1917  
1918  
1919  
1920  
1921  
1922  
1923  
1924  
1925  
1926  
1927  
1928  
1929  
1930  
1931  
1932  
1933  
1934  
1935  
1936  
1937  
1938  
1939  
1940  
1941  
1942  
1943  
1944  
1945  
1946  
1947  
1948  
1949  
1950  
1951  
1952  
1953  
1954  
1955  
1956  
1957  
1958  
1959  
1960  
1961  
1962  
1963  
1964  
1965  
1966  
1967  
1968  
1969  
1970  
1971  
1972  
1973  
1974  
1975  
1976  
1977  
1978  
1979  
1980  
1981  
1982  
1983  
1984  
1985  
1986  
1987  
1988  
1989  
1990  
1991  
1992  
1993  
1994  
1995  
1996  
1997  
1998  
1999  
2000  
2001  
2002  
2003  
2004  
2005  
2006  
2007  
2008  
2009  
2010  
2011  
2012  
2013  
2014  
2015  
2016  
2017  
2018  
2019  
2020  
2021  
2022  
2023  
2024  
2025  
2026  
2027  
2028  
2029  
2030  
2031  
2032  
2033  
2034  
2035  
2036  
2037  
2038  
2039  
2040  
2041  
2042  
2043  
2044  
2045  
2046  
2047  
2048  
2049  
2050  
2051  
2052  
2053  
2054  
2055  
2056  
2057  
2058  
2059  
2060  
2061  
2062  
2063  
2064  
2065  
2066  
2067  
2068  
2069  
2070  
2071  
2072  
2073  
2074  
2075  
2076  
2077  
2078  
2079  
2080  
2081  
2082  
2083  
2084  
2085  
2086  
2087  
2088  
2089  
2090  
2091  
2092  
2093  
2094  
2095  
2096  
2097  
2098  
2099  
2100  
2101  
2102  
2103  
2104  
2105  
2106  
2107  
2108  
2109  
2110  
2111  
2112  
2113  
2114  
2115  
2116  
2117  
2118  
2119  
2120  
2121  
2122  
2123  
2124  
2125  
2126  
2127  
2128  
2129  
2130  
2131  
2132  
2133  
2134  
2135  
2136  
2137  
2138  
2139  
2140  
2141  
2142  
2143  
2144  
2145  
2146  
2147  
2148  
2149  
2150  
2151  
2152  
2153  
2154  
2155  
2156  
2157  
2158  
2159  
2160  
2161  
2162  
2163  
2164  
2165  
2166  
2167  
2168  
2169  
2170  
2171  
2172  
2173  
2174  
2175  
2176  
2177  
2178  
2179  
21

-25-

18. A method comprising:  
obtaining an authentication key; and  
sending a join request to a designated device using a predetermined multicast group management protocol, the join request including the authentication key.

5

19. The method of claim 18, wherein the predetermined multicast group management protocol is an extended Internet Group Management Protocol (IGMP) including means for including the authentication key in the join request.

18. A method comprising:  
obtaining an authentication key; and  
sending a join request to a designated device using a predetermined multicast group management protocol, the join request including the authentication key.

21. The apparatus of claim 20, wherein the predetermined multicast group management protocol is an extended Internet Group Management Protocol (IGMP) including means for including the authentication key in the join request.

-27-

22. A computer readable medium having embodied therein a computer program for controlling a computer system, the computer program comprising:

receiving logic programmed to receive an authentication key; and

group management logic programmed to send a join request to a designated device

using a predetermined multicast group management protocol, the join request including the authentication key.

23. The computer readable medium of claim 22, wherein the predetermined multicast group management protocol is an extended Internet Group Management Protocol (IGMP) including means for including the authentication key in the join request.

24. The computer readable medium of claim 22, wherein the computer readable medium is a computer storage medium.

25. The computer readable medium of claim 22, wherein the computer readable medium is a computer communication medium.



-28-

26. A method comprising:  
receiving a join request from a host device;  
generating an encoded join request using an authentication key associated with the  
host device; and

5 sending the encoded join request toward a rendezvous point device.

27. The method of claim 26, wherein the join request includes the authentication key.

28. The method of claim 26, further comprising:  
joining a shared tree on behalf of the host device and establishing appropriate  
multicast routes for forwarding multicast communication messages to the host device.

10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50  
51  
52  
53  
54  
55  
56  
57  
58  
59  
60  
61  
62  
63  
64  
65  
66  
67  
68  
69  
70  
71  
72  
73  
74  
75  
76  
77  
78  
79  
80  
81  
82  
83  
84  
85  
86  
87  
88  
89  
90  
91  
92  
93  
94  
95  
96  
97  
98  
99  
100  
101  
102  
103  
104  
105  
106  
107  
108  
109  
110  
111  
112  
113  
114  
115  
116  
117  
118  
119  
120  
121  
122  
123  
124  
125  
126  
127  
128  
129  
130  
131  
132  
133  
134  
135  
136  
137  
138  
139  
140  
141  
142  
143  
144  
145  
146  
147  
148  
149  
150  
151  
152  
153  
154  
155  
156  
157  
158  
159  
160  
161  
162  
163  
164  
165  
166  
167  
168  
169  
170  
171  
172  
173  
174  
175  
176  
177  
178  
179  
180  
181  
182  
183  
184  
185  
186  
187  
188  
189  
190  
191  
192  
193  
194  
195  
196  
197  
198  
199  
200  
201  
202  
203  
204  
205  
206  
207  
208  
209  
210  
211  
212  
213  
214  
215  
216  
217  
218  
219  
220  
221  
222  
223  
224  
225  
226  
227  
228  
229  
230  
231  
232  
233  
234  
235  
236  
237  
238  
239  
240  
241  
242  
243  
244  
245  
246  
247  
248  
249  
250  
251  
252  
253  
254  
255  
256  
257  
258  
259  
260  
261  
262  
263  
264  
265  
266  
267  
268  
269  
270  
271  
272  
273  
274  
275  
276  
277  
278  
279  
280  
281  
282  
283  
284  
285  
286  
287  
288  
289  
290  
291  
292  
293  
294  
295  
296  
297  
298  
299  
300  
301  
302  
303  
304  
305  
306  
307  
308  
309  
310  
311  
312  
313  
314  
315  
316  
317  
318  
319  
320  
321  
322  
323  
324  
325  
326  
327  
328  
329  
330  
331  
332  
333  
334  
335  
336  
337  
338  
339  
340  
341  
342  
343  
344  
345  
346  
347  
348  
349  
350  
351  
352  
353  
354  
355  
356  
357  
358  
359  
360  
361  
362  
363  
364  
365  
366  
367  
368  
369  
370  
371  
372  
373  
374  
375  
376  
377  
378  
379  
380  
381  
382  
383  
384  
385  
386  
387  
388  
389  
390  
391  
392  
393  
394  
395  
396  
397  
398  
399  
400  
401  
402  
403  
404  
405  
406  
407  
408  
409  
410  
411  
412  
413  
414  
415  
416  
417  
418  
419  
420  
421  
422  
423  
424  
425  
426  
427  
428  
429  
430  
431  
432  
433  
434  
435  
436  
437  
438  
439  
440  
441  
442  
443  
444  
445  
446  
447  
448  
449  
450  
451  
452  
453  
454  
455  
456  
457  
458  
459  
460  
461  
462  
463  
464  
465  
466  
467  
468  
469  
470  
471  
472  
473  
474  
475  
476  
477  
478  
479  
480  
481  
482  
483  
484  
485  
486  
487  
488  
489  
490  
491  
492  
493  
494  
495  
496  
497  
498  
499  
500  
501  
502  
503  
504  
505  
506  
507  
508  
509  
510  
511  
512  
513  
514  
515  
516  
517  
518  
519  
520  
521  
522  
523  
524  
525  
526  
527  
528  
529  
530  
531  
532  
533  
534  
535  
536  
537  
538  
539  
540  
541  
542  
543  
544  
545  
546  
547  
548  
549  
550  
551  
552  
553  
554  
555  
556  
557  
558  
559  
560  
561  
562  
563  
564  
565  
566  
567  
568  
569  
570  
571  
572  
573  
574  
575  
576  
577  
578  
579  
580  
581  
582  
583  
584  
585  
586  
587  
588  
589  
590  
591  
592  
593  
594  
595  
596  
597  
598  
599  
600  
601  
602  
603  
604  
605  
606  
607  
608  
609  
610  
611  
612  
613  
614  
615  
616  
617  
618  
619  
620  
621  
622  
623  
624  
625  
626  
627  
628  
629  
630  
631  
632  
633  
634  
635  
636  
637  
638  
639  
640  
641  
642  
643  
644  
645  
646  
647  
648  
649  
650  
651  
652  
653  
654  
655  
656  
657  
658  
659  
660  
661  
662  
663  
664  
665  
666  
667  
668  
669  
670  
671  
672  
673  
674  
675  
676  
677  
678  
679  
680  
681  
682  
683  
684  
685  
686  
687  
688  
689  
690  
691  
692  
693  
694  
695  
696  
697  
698  
699  
700  
701  
702  
703  
704  
705  
706  
707  
708  
709  
710  
711  
712  
713  
714  
715  
716  
717  
718  
719  
720  
721  
722  
723  
724  
725  
726  
727  
728  
729  
730  
731  
732  
733  
734  
735  
736  
737  
738  
739  
740  
741  
742  
743  
744  
745  
746  
747  
748  
749  
750  
751  
752  
753  
754  
755  
756  
757  
758  
759  
760  
761  
762  
763  
764  
765  
766  
767  
768  
769  
770  
771  
772  
773  
774  
775  
776  
777  
778  
779  
780  
781  
782  
783  
784  
785  
786  
787  
788  
789  
790  
791  
792  
793  
794  
795  
796  
797  
798  
799  
800  
801  
802  
803  
804  
805  
806  
807  
808  
809  
810  
811  
812  
813  
814  
815  
816  
817  
818  
819  
820  
821  
822  
823  
824  
825  
826  
827  
828  
829  
830  
831  
832  
833  
834  
835  
836  
837  
838  
839  
840  
841  
842  
843  
844  
845  
846  
847  
848  
849  
850  
851  
852  
853  
854  
855  
856  
857  
858  
859  
860  
861  
862  
863  
864  
865  
866  
867  
868  
869  
870  
871  
872  
873  
874  
875  
876  
877  
878  
879  
880  
881  
882  
883  
884  
885  
886  
887  
888  
889  
890  
891  
892  
893  
894  
895  
896  
897  
898  
899  
900  
901  
902  
903  
904  
905  
906  
907  
908  
909  
910  
911  
912  
913  
914  
915  
916  
917  
918  
919  
920  
921  
922  
923  
924  
925  
926  
927  
928  
929  
930  
931  
932  
933  
934  
935  
936  
937  
938  
939  
940  
941  
942  
943  
944  
945  
946  
947  
948  
949  
950  
951  
952  
953  
954  
955  
956  
957  
958  
959  
960  
961  
962  
963  
964  
965  
966  
967  
968  
969  
970  
971  
972  
973  
974  
975  
976  
977  
978  
979  
980  
981  
982  
983  
984  
985  
986  
987  
988  
989  
990  
991  
992  
993  
994  
995  
996  
997  
998  
999  
1000  
1001  
1002  
1003  
1004  
1005  
1006  
1007  
1008  
1009  
1010  
1011  
1012  
1013  
1014  
1015  
1016  
1017  
1018  
1019  
1020  
1021  
1022  
1023  
1024  
1025  
1026  
1027  
1028  
1029  
1030  
1031  
1032  
1033  
1034  
1035  
1036  
1037  
1038  
1039  
1040  
1041  
1042  
1043  
1044  
1045  
1046  
1047  
1048  
1049  
1050  
1051  
1052  
1053  
1054  
1055  
1056  
1057  
1058  
1059  
1060  
1061  
1062  
1063  
1064  
1065  
1066  
1067  
1068  
1069  
1070  
1071  
1072  
1073  
1074  
1075  
1076  
1077  
1078  
1079  
1080  
1081  
1082  
1083  
1084  
1085  
1086  
1087  
1088  
1089  
1090  
1091  
1092  
1093  
1094  
1095  
1096  
1097  
1098  
1099  
1100  
1101  
1102  
1103  
1104  
1105  
1106  
1107  
1108  
1109  
1110  
1111  
1112  
1113  
1114  
1115  
1116  
1117  
1118  
1119  
1120  
1121  
1122  
1123  
1124  
1125  
1126  
1127  
1128  
1129  
1130  
1131  
1132  
1133  
1134  
1135  
1136  
1137  
1138  
1139  
1140  
1141  
1142  
1143  
1144  
1145  
1146  
1147  
1148  
1149  
1150  
1151  
1152  
1153  
1154  
1155  
1156  
1157  
1158  
1159  
1160  
1161  
1162  
1163  
1164  
1165  
1166  
1167  
1168  
1169  
1170  
1171  
1172  
1173  
1174  
1175  
1176  
1177  
1178  
1179  
1180  
1181  
1182  
1183  
1184  
1185  
1186  
1187  
1188  
1189  
1190  
1191  
1192  
1193  
1194  
1195  
1196  
1197  
1198  
1199  
1200  
1201  
1202  
1203  
1204  
1205  
1206  
1207  
1208  
1209  
1210  
1211  
1212  
1213  
1214  
1215  
1216  
1217  
1218  
1219  
1220  
1221  
1222  
1223  
1224  
1225  
1226  
1227  
1228  
1229  
1230  
1231  
1232  
1233  
1234  
1235  
1236  
1237  
1238  
1239  
1240  
1241  
1242  
1243  
1244  
1245  
1246  
1247  
1248  
1249  
1250  
1251  
1252  
1253  
1254  
1255  
1256  
1257  
1258  
1259  
1260  
1261  
1262  
1263  
1264  
1265  
1266  
1267  
1268  
1269  
1270  
1271  
1272  
1273  
1274  
1275  
1276  
1277  
1278  
1279  
1280  
1281  
1282  
1283  
1284  
1285  
1286  
1287  
1288  
1289  
1290  
1291  
1292  
1293  
1294  
1295  
1296  
1297  
1298  
1299  
1300  
1301  
1302  
1303  
1304  
1305  
1306  
1307  
1308  
1309  
1310  
1311  
1312  
1313  
1314  
1315  
1316  
1317  
1318  
1319  
1320  
1321  
1322  
1323  
1324  
1325  
1326  
1327  
1328  
1329  
1330  
1331  
1332  
1333  
1334  
1335  
1336  
1337  
1338  
1339  
1340  
1341  
1342  
1343  
1344  
1345  
1346  
1347  
1348  
1349  
1350  
1351  
1352  
1353  
1354  
1355  
1356  
1357  
1358  
1359  
1360  
1361  
1362  
1363  
1364  
1365  
1366  
1367  
1368  
1369  
1370  
1371  
1372  
1373  
1374  
1375  
1376  
1377  
1378  
1379  
1380  
1381  
1382  
1383  
1384  
1385  
1386  
1387  
1388  
1389  
1390  
1391  
1392  
1393  
1394  
1395  
1396  
1397  
1398  
1399  
1400  
1401  
1402  
1403  
1404  
1405  
1406  
1407  
1408  
1409  
1410  
1411  
1412  
1413  
1414  
1415  
1416  
1417  
1418  
1419  
1420  
1421  
1422  
1423  
1424  
1425  
1426  
1427  
1428  
1429  
1430  
1431  
1432  
1433  
1434  
1435  
1436  
1437  
1438  
1439  
1440  
1441  
1442  
1443  
1444  
1445  
1446  
1447  
1448  
1449  
1450  
1451  
1452  
1453  
1454  
1455  
1456  
1457  
1458  
1459  
1460  
1461  
1462  
1463  
1464  
1465  
1466  
1467  
1468  
1469  
1470  
1471  
1472  
1473  
1474  
1475  
1476  
1477  
1478  
1479  
1480  
1481  
1482  
1483  
1484  
1485  
1486  
1487  
1488  
1489  
1490  
1491  
1492  
1493  
1494  
1495  
1496  
1497  
1498  
1499  
1500  
1501  
1502  
1503  
1504  
1505  
1506  
1507  
1508  
1509  
1510  
1511  
1512  
1513  
1514  
1515  
1516  
1517  
1518  
1519  
1520  
1521  
1522  
1523  
1524  
1525  
1526  
1527  
1528  
1529  
1530  
1531  
1532  
1533  
1534  
1535  
1536  
1537  
1538  
1539  
1540  
1541  
1542  
1543  
1544  
1545  
1546  
1547  
1548  
1549  
1550  
1551  
1552  
1553  
1554  
1555  
1556  
1557  
1558  
1559  
1560  
1561  
1562  
1563  
1564  
1565  
1566  
1567  
1568  
1569  
1570  
1571  
1572  
1573  
1574  
1575  
1576  
1577  
1578  
1579  
1580  
1581  
1582  
1583  
1584  
1585  
1586  
1587  
1588  
1589  
1590  
1591  
1592  
1593  
1594  
1595  
1596  
1597  
1598  
1599  
1600  
1601  
1602  
1603  
1604  
1605  
1606  
1607  
1608  
1609  
1610  
1611  
1612  
1613  
1614  
1615  
1616  
1617  
1618  
1619  
1620  
1621  
1622  
1623  
1624  
1625  
1626  
1627  
1628  
1629  
1630  
1631  
1632  
1633  
1634  
1635  
1636  
1637  
1638  
1639  
1640  
1641  
1642  
1643  
1644  
1645  
1646  
1647  
1648  
1649  
1650  
1651  
1652  
1653  
1654  
1655  
1656  
1657  
1658  
1659  
1660  
1661  
1662  
1663  
1664  
1665  
1666  
1667  
1668  
1669  
1670  
1671  
1672  
1673  
1674  
1675  
1676  
1677  
1678  
1679  
1680  
1681  
1682  
1683  
1684  
1685  
1686  
1687  
1688  
1689  
1690  
1691  
1692  
1693  
1694  
1695  
1696  
1697  
1698  
1699  
1700  
1701  
1702  
1703  
1704  
1705  
1706  
1707  
1708  
1709  
1710  
1711  
1712  
1713  
1714  
1715  
1716  
1717  
1718  
1719  
1720  
1721  
1722  
1723  
1724  
1725  
1726  
1727  
1728  
1729  
1730  
1731  
1732  
1733  
1734  
1735  
1736  
1737  
1738  
1739  
1740  
1741  
1742  
1743  
1744  
1745  
1746  
1747  
1748  
1749  
1750  
1751  
1752  
1753  
1754  
1755  
1756  
1757  
1758  
1759  
1760  
1761  
1762  
1763  
1764  
1765  
1766  
1767  
1768  
1769  
1770  
1771  
1772  
1773  
1774  
1775  
1776  
1777  
1778  
1779  
1780  
1781  
1782  
1783  
1784  
1785  
1786  
1787  
1788  
1789  
1790  
1791  
1792  
1793  
1794  
1795  
1796  
1797  
1798  
1799  
1800  
1801  
1802  
1803  
1804  
1805  
1806  
1807  
1808  
1809  
1810  
1811  
1812  
1813  
1814  
1815  
1816  
1817  
1818  
1819  
1820  
1821  
1822  
1823  
1824  
1825  
1826  
1827  
1828  
1829  
1830  
1831  
1832  
1833  
1834  
1835  
1836  
1837  
1838  
1839  
1840  
1841  
1842  
1843  
1844  
1845  
1846  
1847  
1848  
1849  
1850  
1851  
1852  
1853  
1854  
1855  
1856  
1857  
1858  
1859  
1860  
1861  
1862  
1863  
1864  
1865  
1866  
1867  
1868  
1869  
1870  
1871  
1872  
1873  
1874  
1875  
1876  
1877  
1878  
1879  
1880  
1881  
1882  
1883  
1884  
1885  
1886  
1887  
1888  
1889  
1890  
1891  
1892  
1893  
1894  
1895  
1896  
1897  
1898  
1899  
1900  
1901  
1902  
1903  
1904  
1905  
1906  
1907  
1908  
1909  
1910  
1911  
1912  
1913  
1914  
1915  
1916  
1917  
1918  
1919  
1920  
1921  
1922  
1923  
1924  
1925  
1926  
1927  
1928  
1929  
1930  
1931  
1932  
1933  
1934  
1935  
1936  
1937  
1938  
1939  
1940  
1941  
1942  
1943  
1944  
1945  
1946  
1947  
1948  
1949  
1950  
1951  
1952  
1953  
1954  
1955  
1956  
1957  
1958  
1959  
1960  
1961  
1962  
1963  
1964  
1965  
1966  
1967  
1968  
1969  
1970  
1971  
1972  
1973  
1974  
1975  
1976  
1977  
1978  
1979  
1980  
1981  
1982  
1983  
1984  
1985  
1986  
1987  
1988  
1989  
1990  
1991  
1992  
1993  
1994  
1995  
1996  
1997  
1998  
1999  
2000  
2001  
2002  
2003  
2004  
2005  
2006  
2007  
2008  
2009  
2010  
2011  
2012  
2013  
2014  
2015  
2016  
2017  
2018  
2019  
2020  
2021  
2022  
2023  
2024  
2025  
2026  
2027  
2028  
2029  
2030  
2031  
2032  
2033  
2034  
2035  
2036  
2037  
2038  
2039  
2040  
2041  
2042  
2043  
2044  
2045  
2046  
2047  
2048  
2049  
2050  
2051  
2052  
2053  
2054  
2055  
2056  
2057  
2058  
2059  
2060  
2061  
2062  
2063  
2064  
2065  
2066  
2067  
2068  
2069  
2070  
2071  
2072  
2073  
2074  
2075  
2076  
2077  
2078  
2079  
2080  
2081  
2082  
2083  
2084  
2085  
2086  
2087  
2088  
2089  
2090  
2091  
2092  
2093  
2094  
2095  
2096  
2097  
2098  
2099  
2100  
2101  
2102  
2103  
2104  
2105  
2106  
2107  
2108  
2109  
2110  
2111  
2112  
2113  
2114  
2115  
2116  
2117  
2118  
2119  
2120  
2121  
2122  
2123  
2124  
2125  
2126  
2127  
2128  
2129  
2130  
2131  
2132  
2133  
2134  
2135  
2136  
2137  
2138  
2139  
2140  
2141  
2142  
2143  
2144  
2145  
2146  
2147  
2148  
2149  
2150  
2151  
2152  
2153  
2154  
2155  
2156  
2157  
2158  
2159  
2160  
2161  
2162  
2163  
2164  
2165  
2166  
2167  
2168  
2169  
2170  
2171  
2172  
2173  
2174  
2175  
2176  
2177  
2178  
2179  
2180  
2181  
2182  
2183  
2184  
2185  
2186  
2187  
2188  
2189  
2190  
2191  
2

-29-

29. An apparatus comprising:  
receiving logic operably coupled to receive a join request from a host device;  
encoding logic operably coupled to generate an encoded join request using an  
authentication key associated with the host device; and

5 sending logic operably coupled to send the encoded join request toward a  
rendezvous point device.

30. The apparatus of claim 29, wherein the join request includes the authentication  
key.

31. The apparatus of claim 29, further comprising:  
joining logic operably coupled to join a shared tree on behalf of the host device;  
and

routing logic operably coupled to establish appropriate multicast routes for  
forwarding multicast communication messages to the host device.

-30-

32. A computer readable medium having embodied therein a computer program for controlling a computer system, the computer program comprising:

receiving logic programmed to receive a join request from a host device;

encoding logic programmed to generate an encoded join request using an

5 authentication key associated with the host device; and

sending logic programmed to send the encoded join request toward a rendezvous point device.

33. The computer readable medium of claim 32, wherein the join request includes the authentication key.

34. The computer readable medium of claim 32, further comprising:

joining logic operably coupled to join a shared tree on behalf of the host device;

and

15 routing logic operably coupled to establish appropriate multicast routes for forwarding multicast communication messages to the host device.

35. The computer readable medium of claim 32, wherein the computer readable medium is a computer storage medium.

36. The computer readable medium of claim 32, wherein the computer readable medium is a computer communication medium.

-31-

37. A method comprising:  
receiving an encoded join request for a host device; and  
forwarding the encoded join request toward a rendezvous point device.
- 5 38. The method of claim 37, further comprising:  
joining a shared tree for the host device; and  
establishing appropriate multicast routes for forwarding multicast communication  
messages toward the host device.
- 10 39. The method of claim 37, further comprising:  
waiting for an explicit acknowledgment message from the rendezvous point  
device; and  
establishing appropriate multicast routes for forwarding multicast communication  
messages toward the host device only upon receiving the explicit acknowledgment  
15 message from the rendezvous point device.

-32-

40. An apparatus comprising:

receiving logic operably coupled to receive an encoded join request for a host device; and

forwarding logic operably coupled to forward the encoded join request toward a rendezvous point device.

41. The apparatus of claim 40, further comprising:

joining logic operably coupled to join a shared tree for the host device; and  
routing logic operably coupled to establish appropriate multicast routes for forwarding multicast communication messages toward the host device.

42. The apparatus of claim 40, further comprising:

waiting logic operably coupled to wait for an explicit acknowledgment message from the rendezvous point device; and

routing logic operably coupled to establish appropriate multicast routes for forwarding multicast communication messages toward the host device only upon receiving the explicit acknowledgment message from the rendezvous point device.

-33-

43. A computer readable medium having embodied therein a computer program for controlling a computer system, the computer program comprising:

receiving logic programmed to receive an encoded join request for a host device;

and

forwarding logic programmed to forward the encoded join request toward a rendezvous point device.

44. The computer readable medium of claim 43, further comprising:

joining logic programmed to join a shared tree for the host device; and

routing logic programmed to establish appropriate multicast routes for forwarding multicast communication messages toward the host device.

45. The computer readable medium of claim 43, further comprising:

waiting logic programmed to wait for an explicit acknowledgment message from the rendezvous point device; and

routing logic programmed to establish appropriate multicast routes for forwarding multicast communication messages toward the host device only upon receiving the explicit acknowledgment message from the rendezvous point device.

46. The computer readable medium of claim 43, wherein the computer readable medium is a computer storage medium.

47. The computer readable medium of claim 43, wherein the computer readable medium is a computer communication medium.

-34-

48. A method comprising:  
receiving an encoded join request for a host device;  
authenticating the encoded join request to determine whether or not the encoded  
join request is authentic; and  
5 establishing appropriate multicast routes for forwarding multicast communication  
messages to the host device if and only if the encoded join request is determined to be  
authentic.

49. The method of claim 48, wherein authenticating the encoded join request  
comprises:

10 maintaining a number of authentication keys;  
determining the host device for the encoded join request; and  
searching for an authentication key associated with the host device.

50. The method of claim 49, wherein authenticating the encoded join request further  
comprises:

15 failing to find an authentication key associated with the host device; and  
determining that the encoded join request is not authentic.

51. The method of claim 49, wherein authenticating the encoded join request further  
comprises:

20 finding an authentication key associated with the host device; and  
authenticating the encoded join request using the authentication key associated  
with the host device.

52. The method of claim 48, further comprising:  
25 sending an explicit acknowledgment toward the host device if and only if the  
encoded join request is determined to be authentic.

-35-

53. An apparatus comprising:

receiving logic operably coupled to receive an encoded join request for a host device;

authenticating logic operably coupled to authenticate the encoded join request to determine whether or not the encoded join request is authentic; and

routing logic operably coupled to establish appropriate multicast routes for forwarding multicast communication messages to the host device if and only if the encoded join request is determined to be authentic.

54. The apparatus of claim 53, wherein the authenticating logic is operably coupled to maintain a number of authentication keys, determine the host device for the encoded join request, and search for an authentication key associated with the host device.

55. The apparatus of claim 54, wherein the authenticating logic is operably coupled to determine that the encoded join request is not authentic if the authenticating logic fails to find an authentication key associated with the host device.

56. The apparatus of claim 54, wherein the authenticating logic is operably coupled to authenticate the encoded join request using an authentication key associated with the host device if the authenticating logic finds the authentication key associated with the host device.

57. The apparatus of claim 53, further comprising:

acknowledgment logic operably coupled to send an explicit acknowledgment toward the host device if and only if the encoded join request is determined to be authentic.



58. A computer readable medium having embodied therein a computer program for controlling a computer system, the computer program comprising:

receiving logic programmed to receive an encoded join request for a host device;  
authenticating logic programmed to authenticate the encoded join request to

determine whether or not the encoded join request is authentic; and

routing logic programmed to establish appropriate multicast routes for forwarding multicast communication messages to the host device if and only if the encoded join request is determined to be authentic.

59. The computer readable medium of claim 58, wherein the authenticating logic is programmed to maintain a number of authentication keys, determine the host device for the encoded join request, and search for an authentication key associated with the host device.

60. The computer readable medium of claim 59, wherein the authenticating logic is programmed to determine that the encoded join request is not authentic if the authenticating logic fails to find an authentication key associated with the host device.

61. The computer readable medium of claim 59, wherein the authenticating logic is programmed to authenticate the encoded join request using an authentication key associated with the host device if the authenticating logic finds the authentication key associated with the host device.

62. The computer readable medium of claim 58, further comprising:  
acknowledgment logic programmed to send an explicit acknowledgment toward the host device if and only if the encoded join request is determined to be authentic.

63. The computer readable medium of claim 58, wherein the computer readable medium is a computer storage medium.

-37-

64. The computer readable medium of claim 58, wherein the computer readable medium is a computer communication medium.

64. The computer readable medium of claim 58, wherein the computer readable medium is a computer communication medium.

-38-

65. In a communication system having a host device, a designated device, and a rendezvous point device, a method comprising:

sending a join request by the host device to the designated device in order to join a shared tree;

5 sending an encoded join request by the designated device to the rendezvous point device;

authenticating the encoded join request by the rendezvous point device;

adding the host device to the shared tree, if the encoded join request is authentic;

and

10 excluding the host device from the shared tree, if the encoded join request is not authentic.

-39-

66. A communication message embodied in a data signal, the communication message comprising a group key for a multicast group and an authentication key for a host device.

67. A communication message embodied in a data signal, the communication message comprising a join request including an authentication key for a host device.

68. A communication message embodied in a data signal, the communication message comprising an encoded join request including a tag field and a nonce field.

69. A communication message embodied in a data signal, the communication message comprising an explicit acknowledgment including a tag field and a nonce field.

## ABSTRACT

A system, device, and method for controlling access in a multicast communication network uses a centralized host authentication scheme to prevent unauthorized hosts from joining a shared multicast distribution tree. Each authorized host is allocated a unique authentication key, which is used by the designated router to encode the PIM join message and by the rendezvous point router to authenticate the PIM join message. If the PIM join message is authentic, then each PIM router from the rendezvous point router to the designated router establishes appropriate multicast routes to route multicast packets to the host. If the PIM join message is not authentic, then multicast packets are prevented from reaching the host.

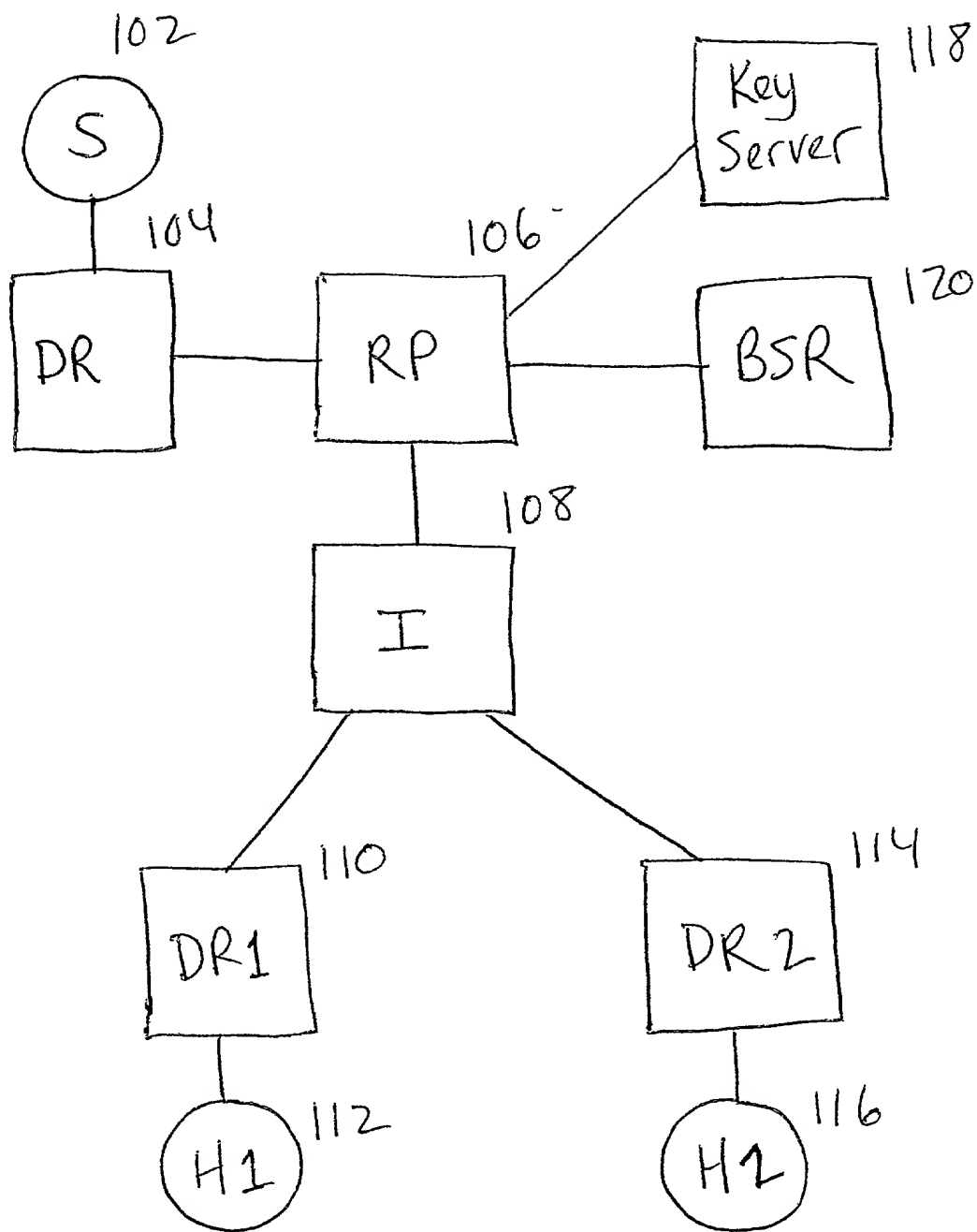


FIG. 1 100

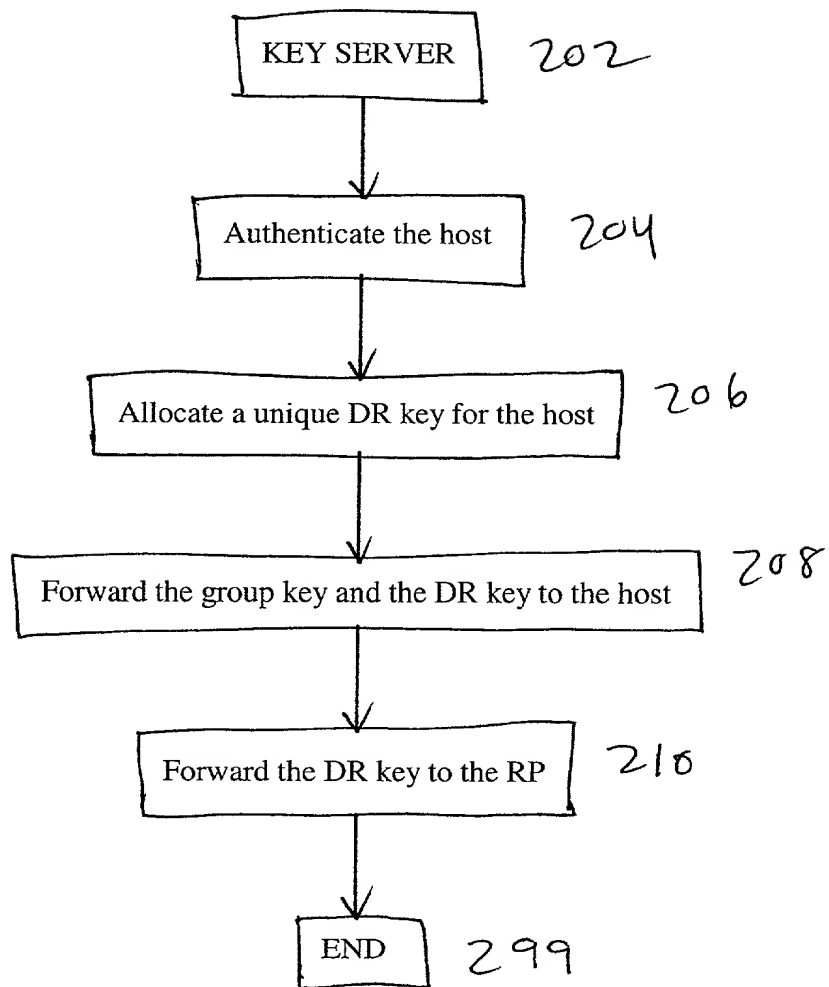


FIG.2 200

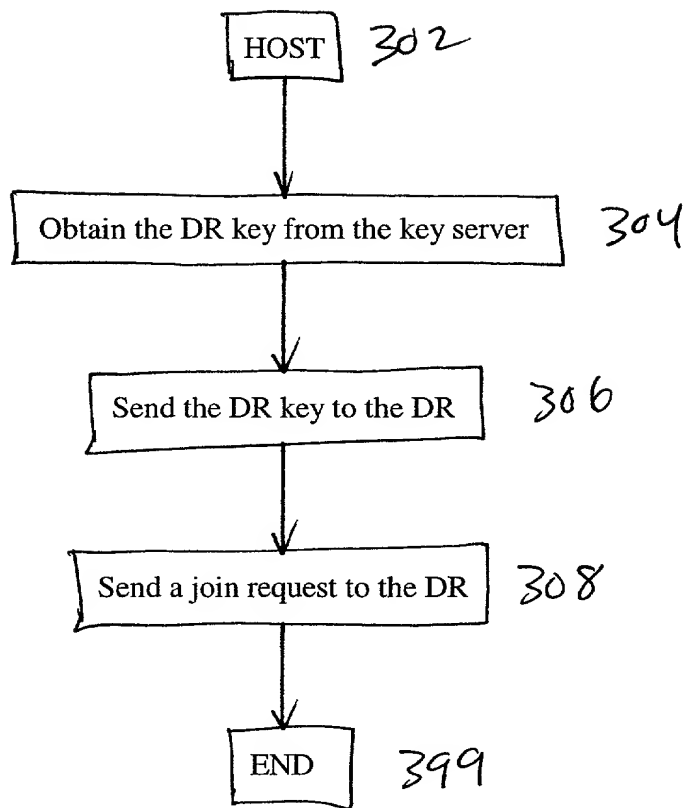


FIG. 3 300



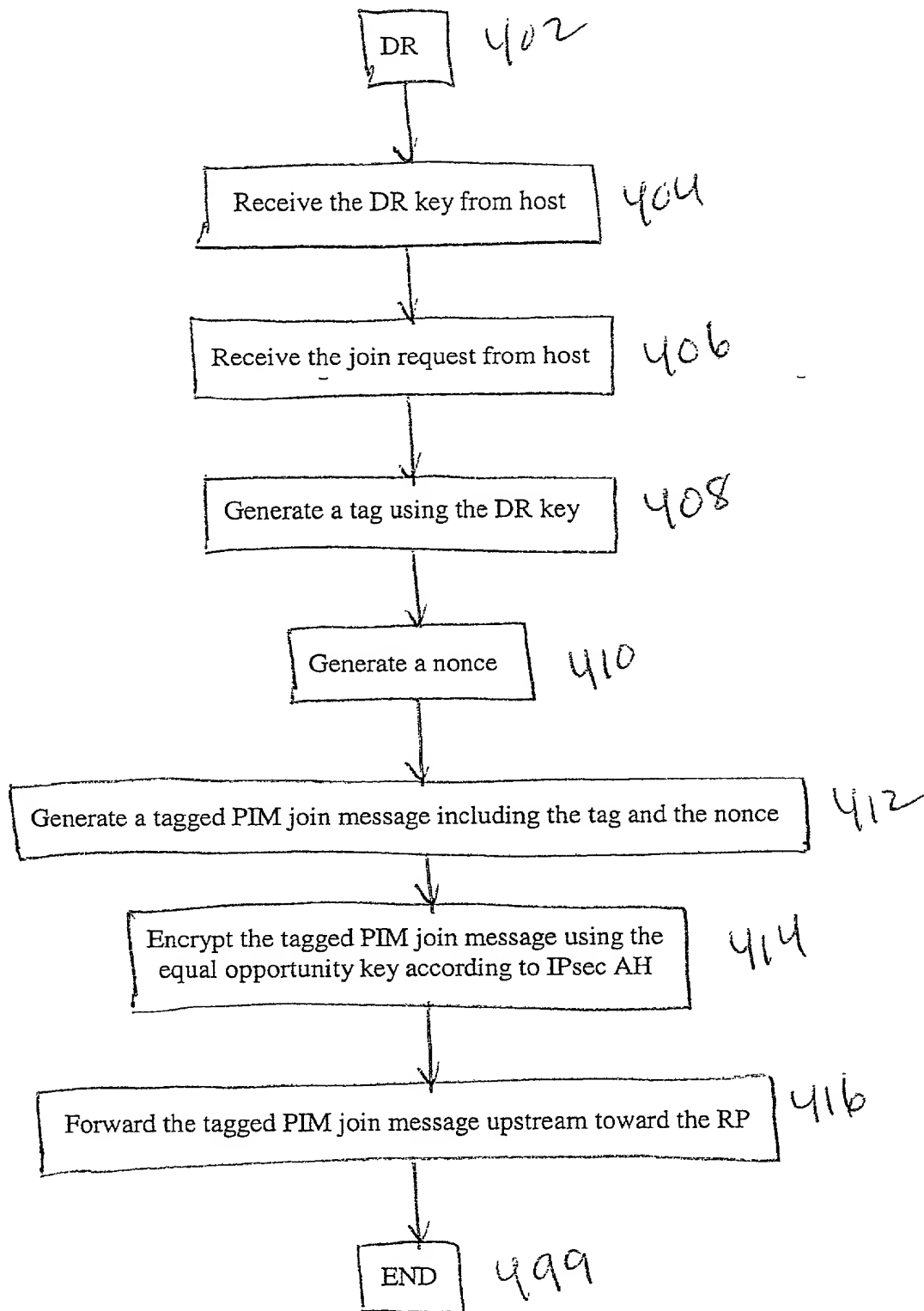


FIG. 4 400

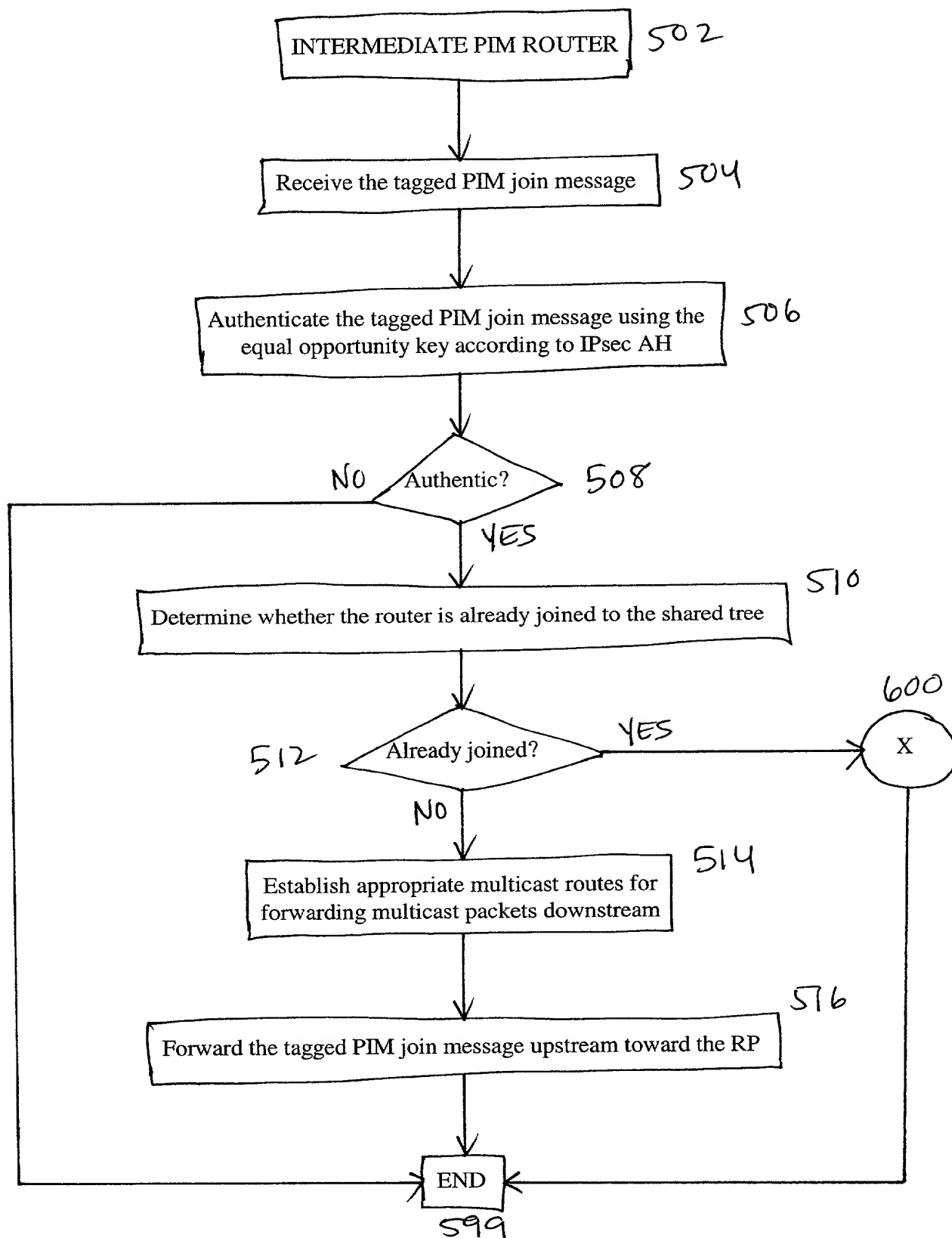


FIG. 5 500

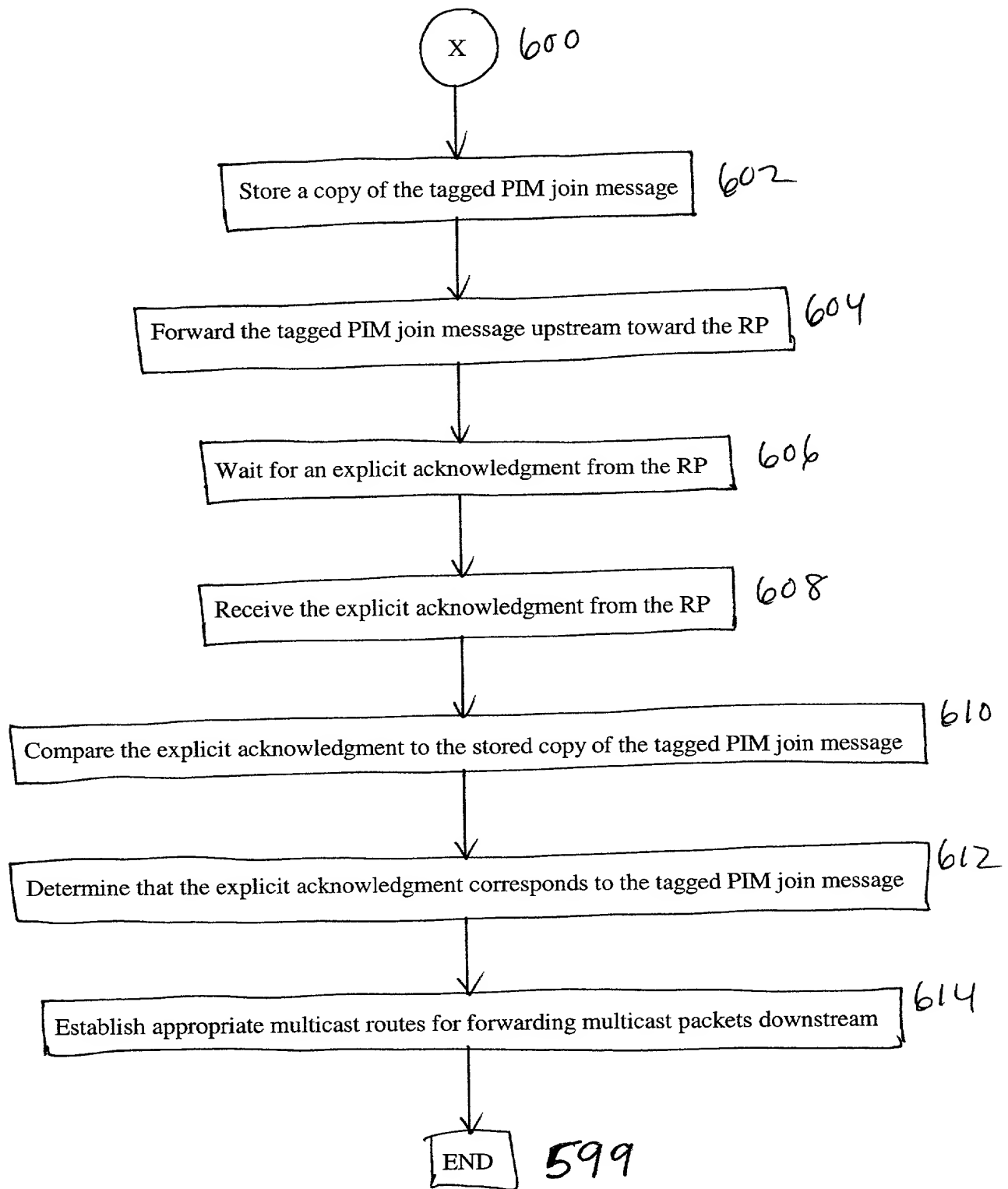


FIG. 6

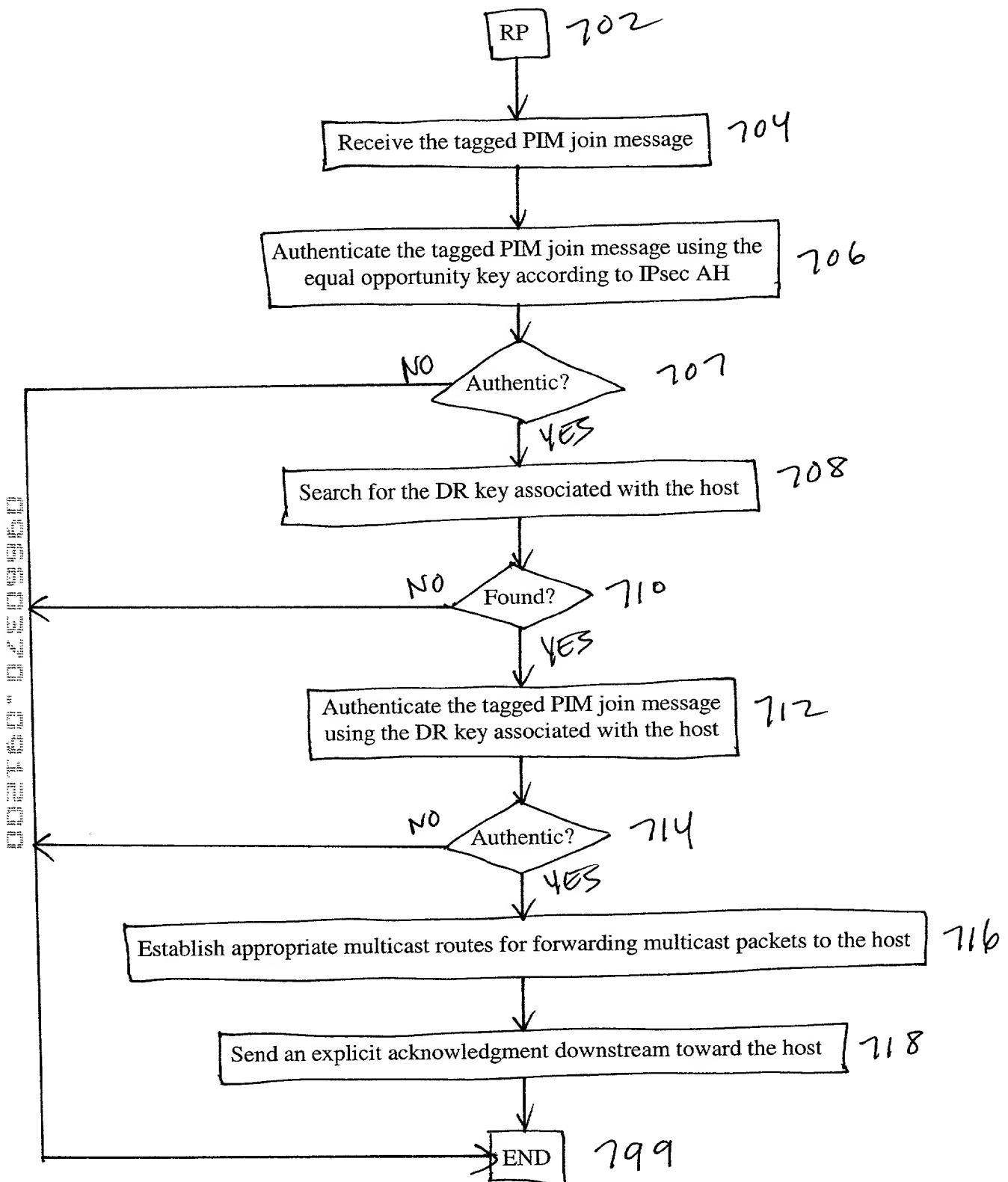


FIG. 7 700



FIG. 8 800

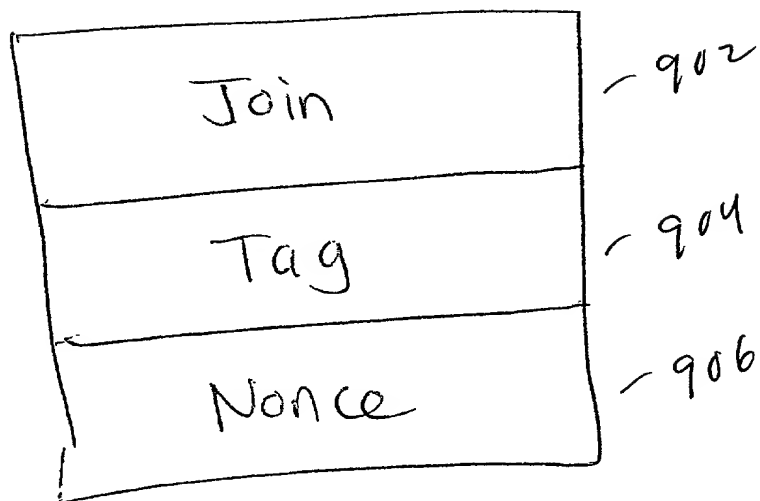


FIG. 9 900

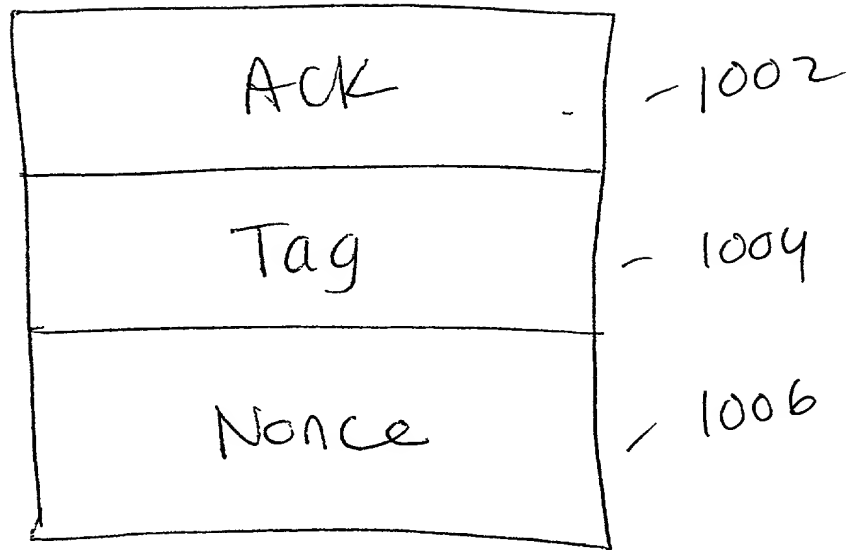


FIG. 10 1000

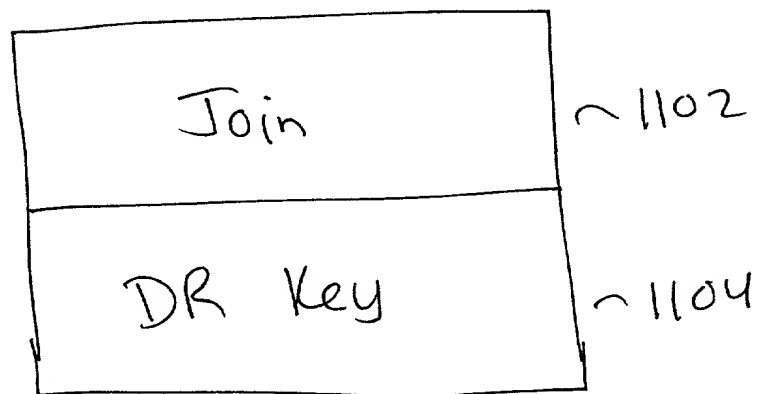


FIG. 11 1100

Docket No.  
2204/A55

# Declaration and Power of Attorney For Patent Application

## English Language Declaration

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name,

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

### SYSTEM, DEVICE, AND METHOD FOR CONTROLLING ACCESS IN A MULTICAST COMMUNICATION NETWORK

the specification of which

(check one)

☒ is attached hereto.

☐ was filed on \_\_\_\_\_ as United States Application No. or PCT International Application Number \_\_\_\_\_ and was amended on \_\_\_\_\_ (if applicable)

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose to the United States Patent and Trademark Office all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, Section 119(a)-(d) or Section 365(b) of any foreign application(s) for patent or inventor's certificate, or Section 365(a) of any PCT International application which designated at least one country other than the United States, listed below and have also identified below, by checking the box, any foreign application for patent or inventor's certificate or PCT International application having a filing date before that of the application on which priority is claimed.

Prior Foreign Application(s)

Priority Not Claimed

(Number)

(Country)

(Day/Month/Year Filed)

☐

(Number)

(Country)

(Day/Month/Year Filed)

☐

(Number)

(Country)

(Day/Month/Year Filed)

☐

I hereby claim the benefit under 35 U.S.C. Section 119(e) of any United States provisional application(s) listed below:

60/204,218

May 15, 2000

(Application Serial No.)

(Filing Date)

(Application Serial No.)

(Filing Date)

(Application Serial No.)

(Filing Date)

I hereby claim the benefit under 35 U. S. C. Section 120 of any United States application(s), or Section 365(c) of any PCT International application designating the United States, listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of 35 U.S.C. Section 112, I acknowledge the duty to disclose to the United States Patent and Trademark Office all information known to me to be material to patentability as defined in Title 37, C. F. R., Section 1.56 which became available between the filing date of the prior application and the national or PCT International filing date of this application:

(Application Serial No.)

(Filing Date)

(Status)  
(patented, pending, abandoned)

(Application Serial No.)

(Filing Date)

(Status)  
(patented, pending, abandoned)

(Application Serial No.)

(Filing Date)

(Status)  
(patented, pending, abandoned)

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.



POWER OF ATTORNEY: As a named inventor, I hereby appoint the following attorney(s) and/or agent(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith. *(list name and registration number)*

Bruce D. Sunstein	Reg. No. 27,234	Jay Sandvos	Reg. No. 43,900
Robert M. Asher	Reg. No. 30,445	Sonia K. Guterman	Reg. No. 44,729
Timothy M. Murphy	Reg. No. 33,198	Keith J. Wood	Reg. No. 45,235
Steven G. Saunders	Reg. No. 36,265	Mary M. Steubing	Reg. No. 37,946
Harriet M. Strimpel	Reg. No. 37,008	Christopher J. Cianciolo	Reg. No. 42,417
Samuel J. Petuchowski	Reg. No. 37,910	Lindsay J. McGuinness	Reg. No. 38,549
Jeffrey T. Klayman	Reg. No. 39,250		
John J. Stickevers	Reg. No. 39,387		
Herbert A. Newborn	Reg. No. 42,031		
Elizabeth P. Morano	Reg. No. 42,904		
Jean M. Tibbetts	Reg. No. 43,193		

Send Correspondence to: **Jeffrey T. Klayman**  
**Bromberg & Sunstein LLP**  
**125 Summer Street**  
**Boston, MA 02110**

Direct Telephone Calls to: *(name and telephone number)*  
**Jeffrey T. Klayman at (617) 443-9292**

Full name of sole or first inventor

**Thomas P. Hardjono**

Sole or first inventor's signature

Date

Residence

**430 Highland Avenue, Winchester, MA 01890**

Citizenship

**Australia**

Post Office Address

**Same as residence**

Full name of second inventor, if any

Second inventor's signature

Date

Residence

Citizenship

Post Office Address